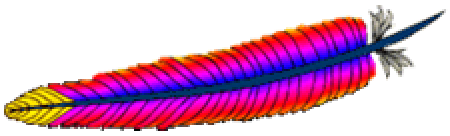
Snort Install Manual



Snort, Apache, PHP, MySQL and Acid Install on RH9.0

By Patrick Harper, CISSP

http://www.InternetSecurityGuru.com

ACID: Analysis Console for Intrusion Detection

Introduction:

This document originated when a friend of mine asked me to put together this procedure for him so that he could install Snort and Acid. It is pretty basic and is for the Linux newbie, as well the snort newbie. This is not an ultra-secure end-all to Snort IDS deployment guide; this is a "How in the hell do I get this installed and working" guide. This document will walk you through installing a stand alone RedHat system (this is not for a dual boot system).

For text editors I would suggest using pico, it is very easy to use (it is part of the pine mail package). Type "pico <filename>" and it will open the file in the editor; all the commands are listed on the bottom. (Remember the ^ is for ctrl)

I have also added a troubleshooting section at the bottom of this document

Acknowledgments:

I would like to thank all my friends and the people on the snort-users list that proofed this for me. First of all, to my wife Kris, who puts up with me and my ever expanding lab. A special thanks to Nick Oliver. He downloaded and used the first document I wrote and volunteered to do test installs and proof the spelling and punctuation for this document. He has become quite proficient with Linux and snort in the past few months. Without him and his valuable input this document would not be as complete as it is. Also a great thanks to the Snort team, where would we be without you.

Comments or Corrections:

Please e-mail any comments or corrections to mailto:Patrick@internetsecurityguru.com

Nick Oliver has also made himself available for contact if for any reason I may be unavailable or running behind on my large and ever growing inbox. mailto:nwoliver@internetsecurityguru.com

The latest version of this document may be found at, **Please use the most up to date version** http://www.internetsecurityguru.com/documents/ I will do my best to keep it updated.

If you follow this doc line by line it will work for you. 90%+ of the e-mails I get are when people miss a step. I always welcome comments and questions and do my best to help when ever I can.

Info for the install:

IP Address	
Subnet Mask	
Gateway	
DNS Servers	
Hostname	

Other important reading:

Snort users manual http://www.snort.org/docs/writing_rules/
Snort FAQ http://www.snort.org/docs/faq.html
The snort user's mailing list http://lists.sourceforge.net/lists/listinfo/snort-users
(The place to get help AFTER you read the FAQ, ALL the documentation on the Snort website, AND have searched Google).
Also make sure to read the link below, before sending questions, so you know the rules. ☺
The Snort drinking game
http://www.theadamsfamily.net/~erek/snort/drinking_game.txt (Thanks Erek)
ACID FAQ http://www.andrew.cmu.edu/~rdanyliw/snort/acid_faq.html
ACID install guide http://www.andrew.cmu.edu/~rdanyliw/snort/acid_config.html
RedHat Support documents for version 9 -
http://www.redhat.com/support/resources/howto/rhl9.html

Websites to visit:
http://www.snort.org
http://www.cert.org/kb/acid/
http://www.mysql.com
http://www.php.net
http://www.redhat.com
http://www.chiark.greenend.org.uk/~sgtatham/putty/ (the putty ssh client)
http://www.bastille-linux.org (Hardening scripts for UNIX and Linux)
http://www.internetsecurityguru.com (my website)

Installing RedHat 9:

We will install a minimal number of packages, sufficient for a usable system. After the install we'll turn off anything that is not needed. It is an ideal dedicated IDS by hardening the OS and further securing the system. It is, however, also a system that can easily be added to for other uses. There are lots of good articles on how to secure a RedHat box on the web. Just go to http://www.google.com and search for "securing redhat".

Welcome:
Click next

Language:
English

Keyboard:
U.S. English

Mouse Configuration:
I always use the generic drivers for my mice (PS/2 or USB, depending on the system), but I am almost always working on a KVM. If you are on a KVM, use the generic drivers. If not, see if your mouse is on the list.

Install Type:
Choose custom

Disk Partitioning:
Choose to automatically partition the hard drive
Choose to remove all partitions from this hard drive (I am assuming that this not a dual boot box)
Make sure the review button is checked
The following is approximately how RedHat will set it up:
SWAP is twice the amount of ram
/boot is about 100 Meg
/ is the rest of the hard drive

Boot Loader:
Go with the default (if this is a dual boot system then go to google and search for info on how to install grub for dual booting)

Network Configuration:
Hit edit
Uncheck "Configure with DHCP"
Leave "Activate on boot"
Set a static IP and subnet mask for your network
Manually set the hostname
Then set a gateway and DNS address's

Always try to assign a static IP address here. I think it is best not to run Snort off of a Dynamic IP, however, if you need to, go ahead and do it, just make sure to point your $HOME_NET variable in your snort.conf to the interface name. You can get more info on that in the Snort FAQ. If this is a dedicated IDS then you do not need to have an IP on the interface that snort is monitoring (this is not covered in this document but there is lots of info on how to do that out on the web).

Firewall:
Security Level - Leave the default at Medium
Choose "Customize"
Trusted devices = BLANK
"Allow Incoming" SSH and WWW" and port 443 only

Additional Language:
Choose only US English

Time Setup:
Choose the closest city within your time zone

Root Password:
Set a strong root password here (a strong password has at least 8 characters with a combination of upper case, lower case, numbers and symbols. It will also not be or resemble anything that might be found in a dictionary of any language)

Authentication:
Use both MD5 and Shadow passwords (the default)
Leave the others as they are

Suggested Packages:
Take the defaults with the following exceptions. (Default is what ever it has when you choose custom; for example, gnome is checked by default and kde is not)

Desktops:
X Window System – click "details" and uncheck the following

- xisdnload (unless you are going to be directly connected to an ISDN line and want this)

Gnome Desktop Environment – Accept the default (checked)

KDE Desktop Environment - Accept the default (unchecked)

Applications:
Editors – Choose your favorites (pico is a very easy to use editor and is installed with the pine mail reader)

Engineering and Scientific – Accept the default (unchecked)

Graphical Internet – check this one and click "details". Install only the following:

- evolution if you want to check e-mail with an Outlook-like client in X
- Mozilla
- Mozilla-psm

Text based internet – check this one and click "details". Install only the following:

- Lynx – a text based web browser
- Pine – a text based e-mail client

Office/Productivity – Only xpdf should be selected

Sound and Video – None of this is needed

Authoring and Publishing – None of this is needed

Graphics – check this one and click "details". Check the following:

- Gimp – good to have if your using gnome
- Gimp data extras
- Gimp print plugin

Games and Entertainment – None of this is needed

Server Section:
Choose nothing from this entire section

Development:
Development tools – check this one and click "details" and check the following in addition to what is checked by default

- Expect
- Gcc-objc

Kernel development – check this one, everything is selected by default

X Software Development – check this one and click "details" and unselect everything under "optional packages"

Gnome Software Development – Leave this unchecked

KDE Software Development – Leave this unchecked

System:
Administration – Leave this unchecked

System Tools – check this one and click "details" and check only the following (some will need to be unchecked)

- Ethereal
- Ethereal gnome
- Nmap
- Nmap frontend

Printing support – Uncheck this (unless you need printing from this machine, then configure as needed)

Miscellaneous:
Choose nothing from this entire section

Remember - Do not install Apache, PHP or MySQL, we will install these from source. You will be walked through every step.

Hit next, then next again
The install will start. First it will format the drive(s) and then it will install the packages. This will take a little while, depending on the speed of the system you're on, so putting on a pot of coffee is good right about here.

Installing extra software:
You can install almost anything, as long as it is not in the servers section of the package's page. Remember, however, that if this system is located outside your firewall, is your production IDS, or if you want it really secure, you will need to install the least amount of software possible.

Each piece of software you install and forget to update and maintain is a vulnerability waiting to happen, and that goes for all systems. To me this is one of the biggest rules for systems administration. Make sure you know what you have, and make sure you keep it patched so you do not contribute to the next worm or virus that threatens to shut down major portions of the internet.

If this is a system you are using to learn Snort, Linux, and all the other cool Linux type things, and is not directly connected to the Internet (i.e. NAT'd behind a firewall/Router), then just have fun. Linux is a great operating system, and it can fully replace a Windows desktop or server. The 3 RedHat 9 CD's (as well as most other distributions) are all you need, right there, and they are free.

If this is a production system, please make sure you learn how to secure it.

After the packages install:

Boot Disk Creation:
Choose no

X Configuration:
Choose your card, monitor, and then the resolution and color depth you desire. Most everything I have used in the past few years is supported. (NOTE: In RedHat 9 you can no longer test your settings before continuing).

Congratulations:
Hit the exit button and the system will reboot.

After the reboot:

Welcome screen:
Click forward

User Account:
Add a user account for yourself here; make sure to give it a strong password

The root account should not be used for everyday use, if you need access to root functions then you can "su-" or "sudo" for root access.

Date and Time:
Set your date, time, time zone, as well as your NTP server, if you have one.

Sound card:
If you have a sound card and will be using it then you can test here, otherwise it will not be needed and can be skipped

Red Hat Network:
Register your system with RHN here so that you will be updated when new patches come out. To do this now you have to update up2date first. Here is how to do that

Go to http://rhn.redhat.com/help/latest-up2date.pxt and download the files for RedHat 9

Then go to the directory where you downloaded the files, and as root execute the following command

rpm -Fvh up2date-*

Now that up2date is updated, you can update the rest of your system

Right click on the RHN icon next to the clock on the toolbar (It should be check mark in a circle)

Choose configuration
Hit forward, hit forward again, and again, and then apply.

It will turn green when it is communicating with RHN, then it will be an oscillating red explanation mark.

Click in the Red **!**, and then hit the "Register with RHN" button.

Hit forward, and forward, and then enter the info for your new account and hit forward.

Then enter your personal info if you want, or just hit forward like me. It will show you the Profile name; it will be the name of your system. Hit forward.

Then you will see all the packages that you need to have updated (the select all packages should be checked, if not check it). Hit forward, then forward, then forward (always upgrade your kernel if it is available). This will take a while. Take a break ☺

You are now being upgraded to the latest and greatest version of everything. If you had a kernel update in here you should reboot. But if you want to save time wait until you download everything (see the bottom of the paper for a shortcut to doing that) and

reconfigure SSH, and select what services you do not need anymore. When it is done hit forward and it will start to install the packages you just downloaded.

Hit next, then finish and continue to the next section.

Login to the system (unless you are coming here from the previous section):
Now we need to disable services that you will not need for this system.
First, login as root. Then click on the RedHat on the bottom left of the toolbar. Select System Settings, then Server Settings, then Services. This will bring up the list of services that start when the system boots up.
Disable the following:
apmd, cups, firstboot, isdn, netfs, nfslock, pcmcia, portmap, sgi_fam

Click on "Save" at the top of that window, and close the service configuration.

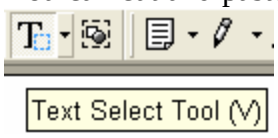
Securing SSH
In the /etc/ssh/sshd_config file change the following lines (if it is commented out, remove the #):
Protocol 2
PermitRootLogin no
PermitEmptyPasswords no

Reboot your system (you installed a new kernel when you updated the installation, and changed the SSH config, so a reboot is necessary). You are now up to date with all the latest packages and you can start the Snort install.

Download all the needed files:

You are now ready to start installing Snort and all of the software it needs. You can either use the desktop terminal window, or SSH into the server from another box, either way will work fine. For the novice it might be easier to do this from SSH so they can cut and paste the commands from this document into the session, instead of typing some of the long strings.

You can cut and paste from the PDF by using the text select tool in Adobe Acrobat



(in doing this sometimes the –'s ands .'s can get messed up, be careful)

Place all the downloaded files into a directory for easy access and consolidation. This directory will not be needed when you are finished with the installation and may be deleted at that time. I create a directory under /root called snortinstall. Use the mkdir command from the shell. Make sure you are in the /root directory (cd /root). You can check where you are currently by using the pwd command. Note: If you are not logged in as root, then you will need to execute "su –" ("su" gives you the super user or root

account rights, the "–" loads the environmental variables of the root account for you) and then enter the root password.

When you are using a Terminal Window, or, if you're SSH'd into the box, you can use wget (wget will place the file you're downloading into the directory where you're currently located) to download these files. To use wget, type "wget <URL_to_file>", and it will begin the download to the directory that you are currently in. If you want to use a Windows box and need an SSH client, then you can go to the PuTTY http://www.chiark.greenend.org.uk/~sgtatham/putty/ home page and download a free one. You can also get a scp (secure copy) and a sftp (Secure FTP) client for Windows there, as well. *(For notes a quick and easy way to download these files, take a look at "download tips" at the end of this paper)*

Download Snort 2.0.4
http://www.snort.org/dl/snort-2.0.4.tar.gz

Download MySQL 4.0.16 Source
http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.16.tar.gz

Download apache 2.0.48
http://www.apache.org/dist/httpd/httpd-2.0.48.tar.gz

Download PHP 4.3.4
http://www.php.net/distributions/php-4.3.4.tar.gz

Download ADODB 4.01
http://phplens.com/lens/dl/adodb401.tgz

Download Acid 0.9.6b23
http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz

Download Zlib 1.1.4
http://flow.dl.sourceforge.net/sourceforge/libpng/zlib-1.1.4.tar.gz

Download JPGraph 1.13
http://www.aditus.nu/jpgraph/downloads/jpgraph-1.13.tar.gz

Download LibPcap 0.7.2
http://www.tcpdump.org/release/libpcap-0.7.2.tar.gz

Preparing for the install:

Again, if you are not logged in as root, then you will need to su to root ("su -" will load the environmental variables of root. Use that when you su.)

Ensure that you have downloaded all of the installation files before you start the install, it will go smoother, trust me. Go to your download directory and start with the following procedures. They will walk you through extracting the source files of the applications, compiling, then installing and configuring them for use with Snort.

(Remember, if you use SSH to access the box, you will need to use the regular user account you created when you installed RH9. Then "su –" to the root account)

Install zlib:

tar -xvzf zlib-1.1.4.tar.gz
cd zlib-1.1.4
./configure; make test
make install
cd ..

Install LibPcap:

tar –xvzf libpcap-0.7.2.tar.gz
cd libpcap-0.7.2
./configure
make
make install
cd ..

Install MySQL:

Create the user and group for MySQL with the following commands:
groupadd mysql
useradd -g mysql mysql

In /root edit the .bash_profile file so the PATH line to read as follows:
PATH=$PATH:$HOME/bin:/usr/local/mysql/bin

Go to the directory you downloaded everything to, and use the following commands to install and configure MySQL.

tar –xvzf mysql-4.0.16.tar.gz
cd mysql-4.0.16
./configure --prefix=/usr/local/mysql
make
make install

scripts/mysql_install_db

chown -R root /usr/local/mysql
chown -R mysql /usr/local/mysql/var

chgrp -R mysql /usr/local/mysql

cp support-files/my-medium.cnf /etc/my.cnf

edit /etc/my.cnf and add the line: user = mysql (this goes in the [mysqld] section

Next, add the lines "/usr/local/mysql/lib/mysql" and "/usr/local/lib" to the /etc/ld.so.conf file.

After you add the lines, run "ldconfig –v", as root

Test to see if it worked:
/usr/local/mysql/bin/mysqld_safe --user=mysql &
(you might have to hit enter to get back to a shell prompt)

If you get no errors, type "ps –ef |grep mysql". You should see something like this:

```
[root@IDS mysql-4.0.16]# ps -ef |grep mysql
root     13297  2290  0 11:20 pts/0    00:00:00 /bin/sh /usr/local/mysql/bin/mysqld_safe --user=mysql
mysql    13319 13297  3 11:20 pts/0    00:00:00 /usr/local/mysql/libexec/mysqld --basedir=/usr/local/mysql
--datadir=/usr/local/mysql/var --user=mysql --pid-file=/usr/local/mysql/var/IDS.pid --skip-locking
```

If it all worked, then go to the next step, which is to make MySQL start when the system boots up.

Set MySQL to start automatically.
Copy the file "mysql.server" from the support-files subfolder (it is under the source for mysql. If you downloaded everything to /root/snortinstall, then the path will be /root/snortinstall/mysql-4.0.16/support-files) to the /etc/init.d folder and call it mysql (the command to copy it from the support-files directory is "cp mysql.server /etc/init.d/mysql")

Use the following commands to create symbolic links in the startup folders for run levels 3 and 5. MySQL will now start automatically when you boot up.

```
cd /etc/rc3.d
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd /etc/rc5.d
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd ../init.d
chmod 755 mysql
```

Installing and configuring Apache with PHP:

This procedure will install the Apache web server in "/www". This is where I prefer to install it. You can, however, modify it for whatever location you wish.

Go back to the download directory and do the following to install Apache and the module for PHP

```
tar -xvzf httpd-2.0.48.tar.gz
cd httpd_2.0.48
./configure --prefix=/www --enable-so
make
make install
```

type "/www/bin/apachectl start"
Check the system to make sure the web server is working (go to the IP of that system in a web browser, you will most likely get an error about the hostname)
type "/www/bin/apachectl stop"

```
cd ..
tar -xvzf php-4.3.4.tar.gz
cd php-4.3.4
```

./configure --prefix=/www/php --with-apxs2=/www/bin/apxs --with-config-file-path=/www/php --enable-sockets --with-mysql=/usr/local/mysql --with-zlib-dir=/usr/local --with-gd (one line)

```
make
make install
```

cp php.ini-dist /www/php/php.ini

Now edit your httpd.conf files (it's in /www/conf) and add:
LoadModule php4_module modules/libphp4.so (The new version of PHP adds it for you)
AddType application/x-httpd-php .php (hit ctrl-w and search for AddType)
DirectoryIndex index.php index.html index.html.var (Search for DirectoryIndex)

IT WILL LOOK SOMETHING LIKE THIS WHEN YOU ARE DONE

```
#
# LoadModule foo_module modules/mod_foo.so
LoadModule php4_module modules/libphp4.so

# AddType allows you to tweak mime.types without actually editing it, or $
# make certain files to be certain types.
#
AddType application/x-tar .tgz
```

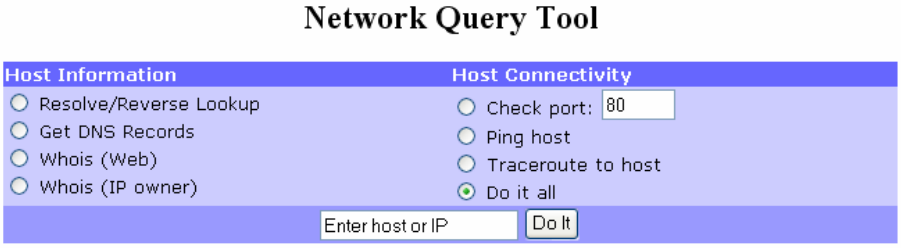
```
AddType image/x-icon .ico
AddType application/x-httpd-php .php

# The index.html.var file (a type-map) is used to deliver content-
# negotiated documents.  The MultiViews Option can be used for the
# same purpose, but it is much slower.
#
DirectoryIndex index.php index.html index.html.var
```

Apache 2.0.48 is now installed in the /www dir. Go into the /www/bin dir and do the following commands:

cp apachectl /etc/init.d/httpd
cd /etc/rc3.d
ln -s ../init.d/httpd S85httpd
ln -s ../init.d/httpd K85httpd
cd /etc/rc5.d
ln -s ../init.d/httpd S85httpd
ln -s ../init.d/httpd K85httpd
(The above lines will add a start up script to the system for both run level 3 and 5)

To test the Apache – PHP install, create a file called test.php in the /www/htdocs directory. Place the following line in the file "<?php phpinfo(); ?>" (without the quotes). Start Apache using "/etc/rc5.d/S85httpd start". Now use a web browser to look at the file (http://IP_Addess/test.php). It should give you info on your system, Apache, and PHP. If you would like another test and a good little tool try using http://shat.net/php/nqt/nqt.php.txt. Copy the text into a file called index.php and place it in the /www/htdocs directory, it will look like the following (just go to the IP in a browser now and you will see it):



Installing and setting up Snort and the Snort rules:

groupadd snort
useradd -g snort snort

mkdir /etc/snort
mkdir /var/log/snort
tar -xvzf snort-2.0.4.tar.gz
cd snort-2.0.4

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

Installing the rules and conf file:
(From the Snort installation directory)
cd rules
cp * /etc/snort
cd ../etc
cp snort.conf /etc/snort
cp *.config /etc/snort

Modify your snort.conf file:
The snort.conf file is located in /etc/snort, make the following changes.

var HOME_NET 10.2.2.0/24 (make this whatever your internal network is)

Change the rule path variable
var RULE_PATH /etc/snort/

Tell it to log to the database (make sure this is on one line) new_password is what ever you want as long as it is the same when you set up mysql

output database: log, mysql, user=snort password=new_password dbname=snort host=localhost

Set snort to start automatically:
Use the script located in the contrib directory, S99snort. Copy it to /etc/init.d and call it snort. (cp contrib/S99snort /etc/init.d/snort) Change the following lines:
CONFIG=/etc/snort/snort.conf
SNORT_GID=snort

Then:
Change directory to /etc/init.d and type:
chmod 755 snort (the file you just edited, or copied from the contrib folder and modified)
cd /etc/rc3.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
cd /etc/rc5.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort

Setting up the database in MySQL:

I will put a line with a > in front of it so you will see what the output should be. (Note: In MySQL, a semi-colon ";" character is mandatory at the end of each input line)
(new_password is whatever password you want to give)

```
/usr/local/mysql/bin/mysql
mysql>  SET PASSWORD FOR root@localhost=PASSWORD('new_password');
>Query OK, 0 rows affected (0.25 sec)
mysql>  create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql>  grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql>  SET PASSWORD FOR snort@localhost=PASSWORD('new_password');
>Query OK, 0 rows affected (0.25 sec)
mysql>  grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql>  grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
>Query OK, 0 rows affected (0.02 sec)
mysql>  exit
>Bye
```

From the Snort 2.0.4 source directory execute the following command (when working with MySQL, if it asks for a password it is wanting the one you defined in the SQL statement "SET PASSWORD FOR root@localhost=PASSWORD('new_password');")

```
/usr/local/mysql/bin/mysql -u root -p  < ./contrib/create_mysql snort
Enter password:
```

Then install the extra DB tables using the following command from the contrib directory (you will need to cd to contrib)

```
zcat snortdb-extra.gz |/usr/local/mysql/bin/mysql -p snort
Enter password:
```

Now you need to check and make sure that the snort DB was created correctly

```
/usr/local/mysql/bin/mysql –p
>Enter password:
mysql>  SHOW DATABASES;
(You should see the following)
+------------+
| Database
+------------+
| mysql
| snort
| test
+------------+
3 rows in set (0.00 sec)
```

```
mysql>  use snort
>Database changed
mysql> SHOW TABLES;
+------------------+
| Tables_in_snort
+------------------+
| data
| detail
| encoding
| event
| flags
| icmphdr
| iphdr
| opt
| protocols
| reference
| reference_system
| schema
| sensor
| services
| sig_class
| sig_reference
| signature
| tcphdr
| udphdr
+------------------+
19 rows in set (0.00 sec)>Bye
```

Install JPGraph:

Go back to your downloads directory

```
cp jpgraph-1.13.tar.gz /www/htdocs
cd /www/htdocs
tar –xvzf jpgraph-1.13.tar.gz
rm –rf jpgraph-1.13.tar.gz
cd jpgraph-1.13
rm -rf README
rm -rf QPL.txt
```

Installing ADODB:

Go back to your download directory

```
cp adodb401.tgz /www/htdocs/
cd /www/htdocs
```

tar -xvzf adodb401.tgz
rm –rf adodb401.tgz

Installing and configuring Acid:

Go back to your downloads directory

cp acid-0.9.6b23.tar.gz /www/htdocs
cd /www/htdocs
tar –xvzf acid-0.9.6b23.tar.gz
rm -rf acid-0.9.6b23.tar.gz

Configuring Acid:
Go to the /www/htdocs/acid/ directory and edit the acid_conf.php file. It should look like this (except of course you will need your password):

```
$DBlib_path = "/www/htdocs/adodb";

/* The type of underlying alert database
 *
 *  MySQL            : "mysql"
 *  PostgresSQL      : "postgres"
 *  MS SQL Server : "mssql"
 */
$DBtype = "mysql";

/* Alert DB connection parameters
 *   - $alert_dbname   : MySQL database name of Snort alert DB
 *   - $alert_host        : host on which the DB is stored
 *   - $alert_port        : port on which to access the DB
 *   - $alert_user        : login to the database with this user
 *   - $alert_password : password of the DB user
 *
 *  This information can be gleaned from the Snort database
 *  output plugin configuration.
 */
$alert_dbname   = "snort";
$alert_host        = "localhost";
$alert_port        = "";
$alert_user        = "snort";
$alert_password = "new_password";

/* Archive DB connection parameters */
$archive_dbname   = "snort";
$archive_host     = "localhost";
$archive_port     = "";
```

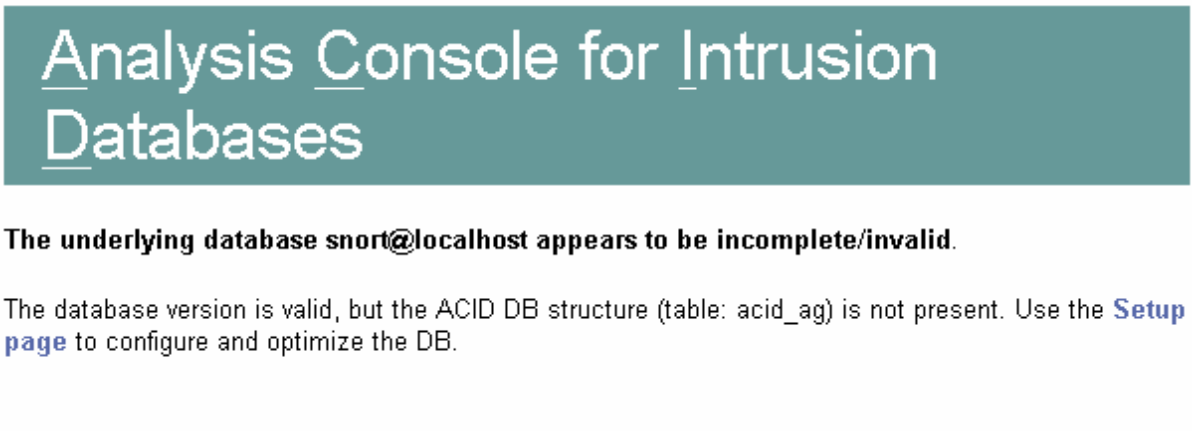
$archive_user = "snort";
$archive_password = 'new_password ";

And a little further down

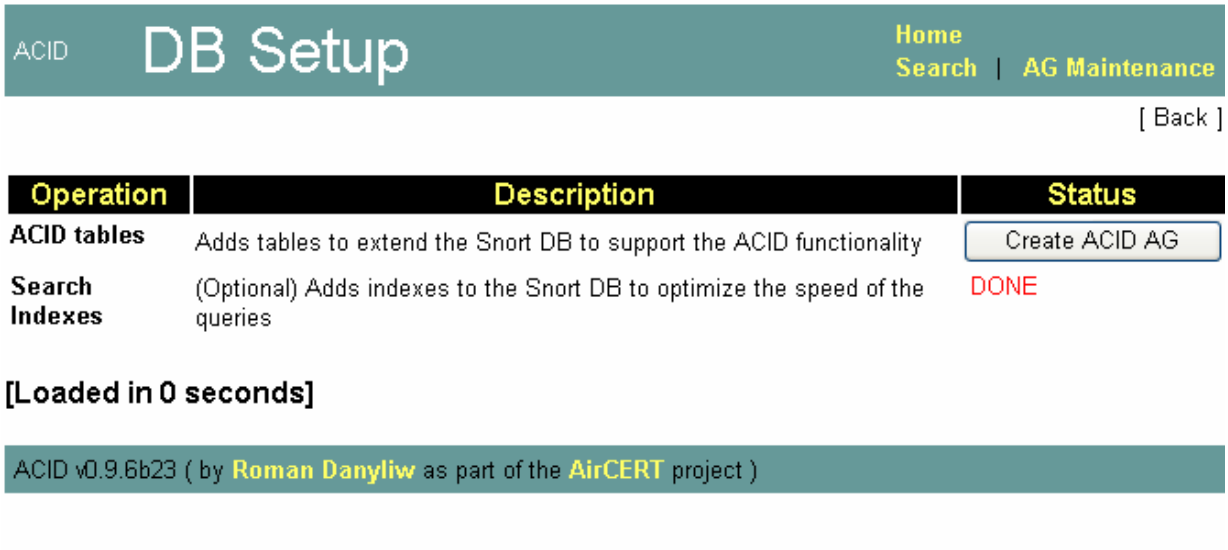
$ChartLib_path = "/www/htdocs/jpgraph-1.13/src";

/* File format of charts ('png', 'jpeg', 'gif') */
$chart_file_format = "png";

Start Apache then go to http://yourhost/acid/acid_main.php . You will get a message that looks like this in your browser:

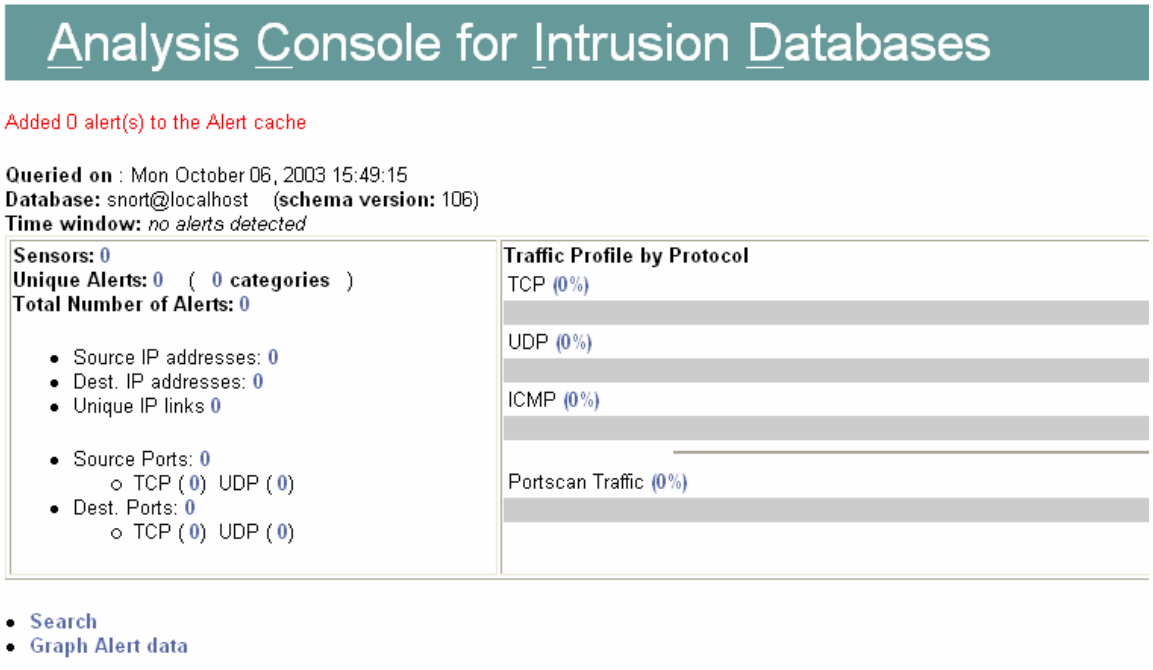


Click on the "Setup Page" hyperlink to create the tables that Acid uses, then you will see the following.



Then click the button that says “Create Acid AG”

Now when you go to http://yourhost/acid/ you should see the ACID homepage



Securing the Acid directory:

mkdir /www/passwords

/www/bin/htpasswd -c /www/passwords/passwords acid

(acid will be the username you will use to get into this directory, along with the password you choose)

It will ask you to enter the password you want for this user, this is what you will have to type when you want to view your acid page

Edit the httpd.conf (/www/conf) and include the following under the section that starts with </Directory>

```
<Directory "/www/htdocs/acid">
    AuthType Basic
    AuthName "SnortIDS"
    AuthUserFile /www/passwords/passwords
    Require user acid
 </Directory>
```

Now restart the http service (/etc/init.d/httpd restart) and next time you go to the acid webpage you will get a prompt for a username and password. (if you are running some of the anti-spyware features of software like spybot search and destroy you will get an error when trying to view this page, or any that require authentication)

Check to see if everything is working:

Reboot your system; watch to make sure everything starts. You can check by doing a "ps –ef |grep <service>" the service can be any running process. i.e. mysql, httpd, snort, etc.

If you want the machine to start at a text prompt instead of X, then change the default in the inittab file (/etc/inittab) from 5 to 3. Go to a shell as root and check everything important to see if it is running.

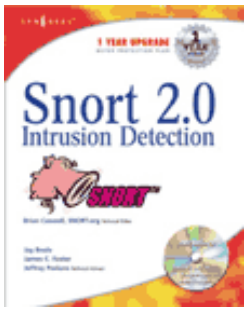
To check you can execute "ps –ef |grep <SERVICE>" where service is snort. httpd, or mysql.

Or use "ps –ef |grep httpd && ps –ef |grep mysql && ps –ef |grep snort"

Now it's time to test snort. I suggest using something free like CIS Scanner (http://www.cerberus-infosec.co.uk/CIS-5.0.02.zip) or Nessus (http://www.nessus.org) if you have it, and running it against your snort box. Check ACID when you're done and it should have a bunch or alerts. If you are on DSL or cable then you could already have a bunch in there right after you start it up. When you go to the acid screen in your browser now you should see alerts (And this is without running any programs against it)

Now you need to tune your IDS for your environment. This is an important step. Look at the Snort list archives and the other links listed above and you will find good tips on how to do that.

There is also a very good book out on Snort for those that want to learn more about it



http://www.amazon.com/exec/obidos/tg/stores/detail/-/books/1931836744/

Download tip

When I want to download all of these real quick I take the following and create a file in the /root/snortinstall dir called get, edit it and put the following in it

```
wget http://www.snort.org/dl/snort-2.0.4.tar.gz
wget http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.16.tar.gz
wget http://www.apache.org/dist/httpd/httpd-2.0.48.tar.gz
wget http://www.php.net/distributions/php-4.3.4.tar.gz
wget http://phplens.com/lens/dl/adodb401.tgz
wget http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz
wget http://flow.dl.sourceforge.net/sourceforge/libpng/zlib-1.1.4.tar.gz
wget http://www.aditus.nu/jpgraph/downloads/jpgraph-1.13.tar.gz
wget http://www.tcpdump.org/release/libpcap-0.7.2.tar.gz
```

Then I save the file and type chmod +x get, then ./get and it will download all the files for me.

Troubleshooting

If you are having trouble type the following
snort –c /etc/snort/snort.conf
It will give you output that will be helpful. It will tell you if you are having problems with rules or if you have a bad line in your conf file. If you do this and read the output you will be able to fix most of the problems we get e-mailed with.

If you are not seeing traffic you need to look at what you have the snort box hooked up to. If you are on a switch you will only see traffic destine for the port you are on (remember not all hubs are real hubs) A true hub will broadcast all traffic to all ports.

If you go to the ip of the snort box in a web browser and send /etc/passwd in the URL and it will trigger an alert if everything is working. (http://ip_address/etc/passwd)

Make sure all services are working, ps –ef |grep <service> (i.e. ps –ef|grep httpd)

Make sure that the line for MySQL in the snort.conf file is not wrapped or cut into two lines. I have seen this happen a lot.

Next, this is an end to end guide. I designed it to take a system from bare metal to functional IDS. If you follow it step by step you will get an IDS working, then you customize it more. I have the RedHat install listed the way I do because there are some parts that are needed.

Most of the problems people have had stem from them missing a step, one step somewhere. There are a lot of them and it is easy to do.

If you do have problems feel free to e-mail me, Nick, or the snort-users list.
There is a huge community of people that use this product that will help you out if you are in trouble.

Good luck and happy snorting.