

# Snort Install Manual



**Snort, Apache, SSL, PHP, MySQL and Acid  
Install on Fedora Core 1 – From Source**

**By Patrick Harper, CISSP, RHCT, MCSE**

<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/Fedora system (this is not for a dual boot system).

For text editors I would suggest using nano, as it is very easy to use. Type “nano <filename>” and it will open the file in the editor. All the commands are listed on the bottom. (Remember that the ^ is for ctrl)

**I have also added a troubleshooting section at the end 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 year. Without him and his valuable input this document would not be as complete as it is. Also a great thanks to Marty and 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 is located at <http://www.internetsecurityguru.com/documents/>. Please try to use the most up to date version I will do my best to keep it updated.

If you follow this doc line by line it will work for you. Over 90% of the e-mails I get are from people who miss a step. However, I always welcome comments and questions and will 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/](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>

*This is 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. It helps to know the rules. ☺*

**The Snort drinking game**

[http://www.theadamsfamily.net/~erek/snort/drinking\\_game.txt](http://www.theadamsfamily.net/~erek/snort/drinking_game.txt) (Thanks EreK)

**ACID FAQ** [http://www.andrew.cmu.edu/~rdanyliw/snort/acid\\_faq.html](http://www.andrew.cmu.edu/~rdanyliw/snort/acid_faq.html)

**ACID install guide** [http://www.andrew.cmu.edu/~rdanyliw/snort/acid\\_config.html](http://www.andrew.cmu.edu/~rdanyliw/snort/acid_config.html)

**RedHat Support documents for Fedora –**

<http://fedora.redhat.com/docs/release-notes/>

### Websites to visit:

<http://www.Snort.org>

<http://www.cert.org/kb/acid/>

<http://www.mysql.com>

<http://www.php.net>

<http://fedora.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 Fedora Core 1:

---

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. By hardening the OS and further securing the system, it will make an ideal dedicated IDS. 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/Fedora box on the web. Just go to <http://www.google.com> and search for "securing redhat" or visit <http://www.bastille-linux.org/>.

**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.

**Monitor Configuration**

Choose your monitor type here, or, if you don't know your monitor characteristics, choose "unprobed Monitor"

**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:**

Leave the default “Enable Firewall”

Choose WWW and SSH only as services to pass through the firewall

Other Ports: 443

Allow traffic from other devices: Leave Blank

**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 should also not be, or resemble, anything that might be found in a dictionary of any language)

**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
- VNC Server

Gnome Desktop Environment – Accept the default (checked)

KDE Desktop Environment - Accept the default (unchecked)

**Applications:**

Editors – Choose your favorites, however, nano is suggested and is part of the base install.

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

Text based internet – check this one and click “[details](#)”. Install only the following:

- elinks – a text based web browser

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 and accept the default 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. It will tell you that you will need all 3 CD's. Hit continue and 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 want 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 most fundamental rules of systems administration. Make sure you know what you have, and make sure you keep it patched and secured so you do not contribute to the next worm, virus, or hacking spree 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 Fedora Core 1 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:**

**Reboot** – hit the reboot button

**After the reboot:**

**Welcome screen:**

Click next

**License Agreement:**

Accept and hit next

**Date and Time:**

Set date and time, hit next.

**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.

**Sound Card:**

You can do this one or just hit next if you want

**Additional CD's:**

Hit next

**Finish Setup:**

Hit next

**Login to the system:**

You should get a graphical login screen now. We need to disable the services that you will not need for this system. First:

Login as root

Click on the RedHat on the bottom left of the toolbar

Select System Settings

Server Settings

Services

This brings up the list of services that start when the system boots up.

Disable the following:

apmd, cups, isdn, netfs, nfslock, pcmcia, portmap, sgi\_fam

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

Click on the red icon next to the clock in the lower right of your screen and go through the prompts to update your system.

Click on the button that says Register with Redhat

There is a tab called “exceptions”. Remove “kernel\*” from this tab, then do the update.

Once the update listing has been received, select only up2date and gnome-up2date

Install these two rpm's and close the update utility.

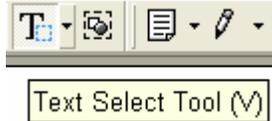
Run the Update feature again, this time with the new Up2date.

Reboot your system (you installed a new kernel when you updated the installation, so a reboot is necessary). You are now up to date with all the latest packages.

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 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



## Download all the needed files:

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.

## !!!DO THE FOLLOWING AS ROOT!!!

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 on quick ways to download see the bottom of this paper)*

Download Snort

<http://www.Snort.org/dl/snort-2.1.2.tar.gz>

Download MySQL Source

<http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.18.tar.gz>

Download Apache

<http://www.apache.org/dist/httpd/httpd-2.0.49.tar.gz>

Download PHP

<http://www.php.net/distributions/php-4.3.4.tar.gz>

Download ADODB

<http://phplens.com/lens/dl/adodb411.tgz>

Download Acid

<http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz>

Download Zlib

<http://www.zlib.net/zlib-1.2.1.tar.gz>

Download JpGraph

<http://www.aditus.nu/jpgraph/downloads/jpgraph-1.14.tar.gz>

Download LibPcap

<http://www.tcpdump.org/release/libpcap-0.8.1.tar.gz>

Download PCRE

<ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-4.4.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.

### **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

(You will need to SSH into the box with the user account you created after this, as root will no longer be accepted. Just "su -" to the root account)

## **Installing PCRE:**

---

```
tar -xvzf pcre-4.4.tar.gz
cd pcre-4.4
./configure
make
make install
```

## **Install zlib:**

---

```
tar -xvzf zlib-1.2.1.tar.gz
cd zlib-1.2.1
./configure; make test
make install
cd ..
```

## **Install LibPcap:**

---

```
tar -xvzf libpcap-0.8.1.tar.gz
cd libpcap-0.8.1
./configure
make
make install
cd ..
```

## **Install MySQL:**

---

Create the user and group for MySQL with the following commands:

```
groupadd mysql
useradd -g mysql mysql -s /dev/null
```

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-4.0.18.tar.gz
cd mysql-4.0.18
./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
```

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@patrick-redhat mysql-4.0.18]# 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/patrick-redhat.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-4.0.18/support-files`) to the `/etc/init.d` folder and call it `mysql`

```
cd /root/snortinstall  
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-2.0.49.tar.gz  
cd httpd_2.0.49
```

```
./configure --prefix=/www --enable-so --enable-ssl --enable-mod_ssl
make
make install
```

```
mkdir /www/certs
cd /www/certs
openssl genrsa -out server.key 1024
openssl req -new -key server.key -x509 -out server.crt
After you type this, fill in the info
```

EDIT SSL.CONF FILE TO POINT TO CERT YOU CREATED

Its location is /www/conf/ssl.conf

Change:

```
SSLCertificateFile /www/conf/ssl.crt/server.crt
```

To

```
SSLCertificateFile /www/certs/server.crt
```

And several lines down, change:

```
SSLCertificateKeyFile /www/conf/ssl.key/server.key
```

To

```
SSLCertificateKeyFile /www/certs/server.key
```

```
type "/www/bin/apachectl startssl"
```

check the system to make sure the web server is working (go to the IP of that system in a web browser. Us both http and https)

```
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, this is where a lot of people mess up, double check to
make sure you have all the right dashes and correct spacing)
```

```
make
```

```
make install
```

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

Now edit your httpd.conf files (it's in /www/conf) and add:

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

```
DirectoryIndex index.php index.html index.html.var
```

.....  
**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

```

```
cp /www/bin/apachectl /etc/init.d/httpd
```

edit the /etc/init.d/httpd file and make the following changes, this will make Apache start with SSL at boot time.

```

start|stop|restart|graceful)
    $HTTPD -k $ARGV
    ERROR=$?
    ;;
startssl|sslstart|start-SSL)

```

**TO**

```

stop|restart|graceful)
    $HTTPD -k $ARGV
    ERROR=$?
    ;;
start|startssl|sslstart|start-SSL)

```

```

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 startup 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(); ?>
```

Start Apache using “/etc/rc5.d/S85httpd start”. Now use a web browser to look at the file ([http://IP\\_Address/test.php](http://IP_Address/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:

### Network Query Tool

Host Information	Host Connectivity
<input type="radio"/> Resolve/Reverse Lookup	<input type="radio"/> Check port: <input type="text" value="80"/>
<input type="radio"/> Get DNS Records	<input type="radio"/> Ping host
<input type="radio"/> Whois (Web)	<input type="radio"/> Traceroute to host
<input type="radio"/> Whois (IP owner)	<input checked="" type="radio"/> Do it all
<input type="text" value="Enter host or IP"/> <input type="button" value="Do It"/>	

## Installing and setting up Snort and the Snort rules:

---

```
groupadd snort
useradd -g snort snort -s /dev/null
```

```
mkdir /etc/snort
mkdir /var/log/snort
mkdir /etc/snort/rules
tar -xvzf snort-2.1.2.tar.gz
cd snort-2.1.2
./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/rules
cd ../etc
cp *.conf /etc/snort
cp *.config /etc/snort
cp *.map /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 what ever your internal network is)
```

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

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 later.

```
output database: log, mysql, user=snort password=new_password dbname=snort
host=localhost (ONE LINE)
```

**Set Snort to start automatically:**

Use the script located in the contrib. It will be the S99snort file. You will copy it to /etc/init.d and call it snort.

```
cd ../contrib
cp S99snort /etc/init.d/snort
```

It should look like the following.

```
# Configuration

# set config file & path to Snort executable
SNORT_PATH=/usr/local/bin
CONFIG=/etc/snort/snort.conf

# set interface
IFACE=eth0

# set GID/Group Name
SNORT_GID=snort

# other options
OPTIONS="-D"

# End of configuration
```

**Then:**

Change directory to /etc/init.d and type:

```
chmod 755 snort (the file you just 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 2.1.1 source directory (/root/snortinstall/snort-2.1.1) 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
| icmp_hdr
| ip_hdr
| opt
| protocols
| reference
| reference_system
| schema
| sensor
| services
| sig_class
| sig_reference
| signature
| tcp_hdr
| udp_hdr
+-----+
19 rows in set (0.00 sec)
exit
```

## **Install JPGraph:**

---

Go back to your downloads directory

```
cp jpgraph-1.14.tar.gz /www/htdocs
cd /www/htdocs
tar -xvzf jpgraph-1.14.tar.gz
rm -rf jpgraph-1.14.tar.gz
cd jpgraph-1.14
rm -rf README
```

## **Installing ADODB:**

---

Go back to your download directory

```
cp adodb411.tgz /www/htdocs/
cd /www/htdocs
```

```
tar -xvzf adodb411.tgz
rm -rf adodb411.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): The highlighted items are what you need to change

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

```
$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-1.14/src";
```

Start Apache (/etc/rc5.d/S85httpd start) then go to [http://yourhost/acid/acid\\_main.php](http://yourhost/acid/acid_main.php) .  
You will get a message that looks like this in your browser:

## Analysis Console for Intrusion Databases

The underlying database snort@localhost appears to be incomplete/invalid.

The database version is valid, but the ACID DB structure (table: acid\_ag) is not present. Use the [Setup page](#) to configure and optimize the DB.

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

ACID **DB Setup** [Home](#) [Search](#) | [AG Maintenance](#) [ Back ]

Operation	Description	Status
<b>ACID tables</b>	Adds tables to extend the Snort DB to support the ACID functionality	<input type="button" value="Create ACID AG"/>
<b>Search Indexes</b>	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

[Loaded in 0 seconds]

ACID v0.9.6b23 ( by [Roman Danyliw](#) as part of the [AirCERT](#) project )

Then click the button that says "Create Acid AG"

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

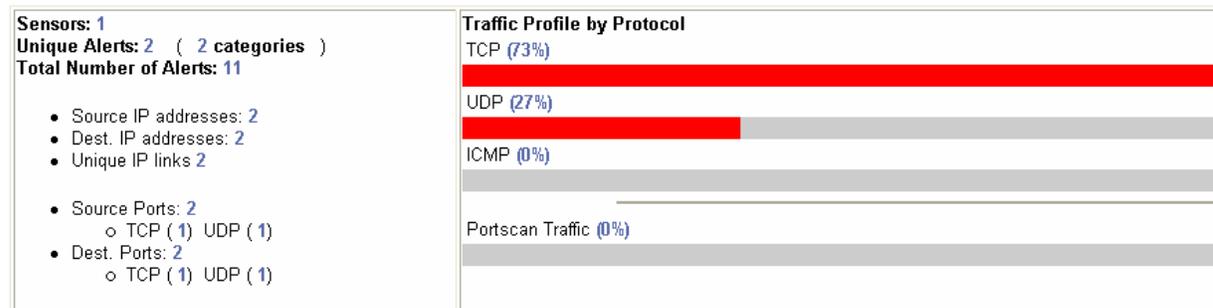
# Analysis Console for Intrusion Databases

Added 0 alert(s) to the Alert cache

Queried on : Fri May 02, 2003 12:47:26

Database: snort@localhost (schema version: 106)

Time window: [2003-05-02 12:46:20] - [2003-05-02 12:46:35]



- [Search](#)
- [Graph Alert data](#)

- **Snapshot**

- Most recent Alerts: [any protocol](#), [TCP](#), [UDP](#), [ICMP](#)
- Today's: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)
- Last 24 Hours: alerts [unique](#), [listing](#); IP [src](#) / [dst](#)

- Most frequent 5 Alerts

- Most Frequent Source Ports: [any](#), [TCP](#), [UDP](#)

## 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 , I put it under the section that has:

```
<Directory />  
Options FollowSymLinks  
AllowOverride None  
</Directory>
```

These are the lines to add:

```
<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.

### **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.

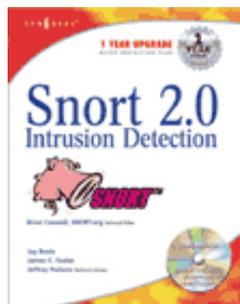
To check you can execute “ps -ef |grep <SERVICE>” where service is Snort. httpd, or mysql.

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 of 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/>

And a few others listed at [http://www.Snort.org/docs/#Snort\\_books](http://www.Snort.org/docs/#Snort_books)

## 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-2.1.1.tar.gz
wget http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.18.tar.gz
wget http://www.apache.org/dist/httpd/httpd-2.0.49.tar.gz
wget http://www.php.net/distributions/php-4.3.4.tar.gz
wget http://phplens.com/lens/dl/adodb411.tgz
wget http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz
wget http://www.zlib.net/zlib-1.2.1.tar.gz
wget http://www.aditus.nu/jpgraph/downloads/jpgraph-1.14.tar.gz
wget http://www.tcpcdump.org/release/libpcap-0.8.1.tar.gz
wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-4.4.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/sort.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 I get e-mailed with.

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.

If you do not have a sensor number, it means that you have not received an alert on that sensor yet. Make sure everything is running without error and check ACID again

If you get errors about libpng, libjpeg, or any other lib item (when you are compiling PHP) you missed them during the install of the OS. Go to system settings (hit the "Redhat" in the bottom left and look for it on the pop up menu), then to add/remove applications and

you can check what you installed. Make sure it is at the minimum what I have listed for the OS install.

If you are getting nothing in ACID you could have a number of problems. Check your /var/log/snort directory and see if you have an alert file. If it has alerts, then Snort is working and you most likely do not have your Snort.conf output lines correct. Check where you setup your database in it first. If you do not have an alert file then make sure Snort is running. If it is, make sure that if you are on a switch, you are on a span (or mirrored) port, or you will not see anything but what is destined for that port.

The best place to look for other answers is the Snort-users archive, which is indexed by Google. If you are not proficient at searching, I would suggest reading <http://www.google.com/help/basics.html> . It is a good primer, as is <http://www.googleguide.com/>

Read what is out there for you. Go to <http://www.snort.org> and look around. [http://www.snort.org/docs/snort\\_manual/](http://www.snort.org/docs/snort_manual/) is also something you should read all the way through, as well as <http://www.snort.org/docs/FAQ.txt> between them and Google almost all your questions will be answered.

Most of the problems people have had stem from them missing a step, frequently only 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 out there using this product that will help you if you are in trouble. Remember, however, that this support is free and done out of love of this product. You certainly should not expect the same response from the Snort community as you would from an IDS vendor (though I have gotten better response time from the Snort-users list than I have from some vendors in the past)

Hope this gets you going. If not, then feel free to e-mail either myself, Nick Oliver, or the Snort-users list. They are a great bunch of people and will do all they can for you (if you have manners). Just remember, however, that it is a volunteer thing, so you will probably not get answers in 10 minutes. Do NOT repost your question merely because you have not yet seen an answer.

Good luck and happy Snorting.