

Snort Installation Manual using Mandrake 9.2

By Nick Duda, CCSE, Security+, CEH, MCP, MCDST

Snort 2.1.0
MySQL 4.0.17
Apache 2.0.48
PHP 4.3.4
ADODB 3.90
ACID 0.9.6b23
ZLIB 1.2.1
JPGGraph 1.14
LibPcap 0.8.1
Swatch 3.0.8
Webmin 1.121



Introduction:

Recently I've seen numerous requests in message forums on installing and running Snort using Mandrake. Inspired by the Snort Installation sheet by Patrick Harper, I've decided to dedicate this document to a similar install but taking it to the next step, getting it up and running in a real environment with email alerting. As Patrick Harper wisely puts it, this document is for the Linux/Snort newbie and is meant as a general guide to "How in the hell do I get this installed and working".

Comments or Corrections:

I can be contacted at nduda78@comcast.net for any comments, corrections, feedback (good or bad, just go easy on the bad).

Configuration:

This document will take you step by step through a Mandrake 9.2 install with Snort, Apache, PHP, MySQL, ACID, Webmin and Swatch (and additional components as needed).

We will build this Snort box to actively monitor the segment connected to eth0 (promiscuous mode). This can be a spanned switch/hub port (figure 1), or any single device (figure 2) you choose to monitor or even be configured right on an IPTables (firewall) box (figure 3). It will also talk to the Local Area Network on eth1. Once up and running, we will configure the ACID interface, Webmin module and Swatch to send you email alerts when a signature is triggered.

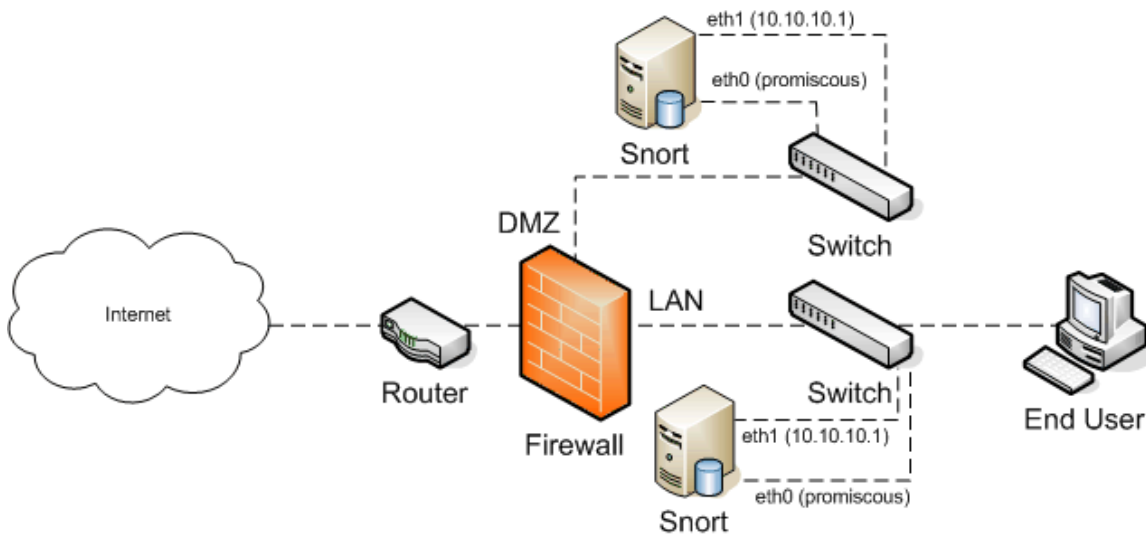


Figure 1

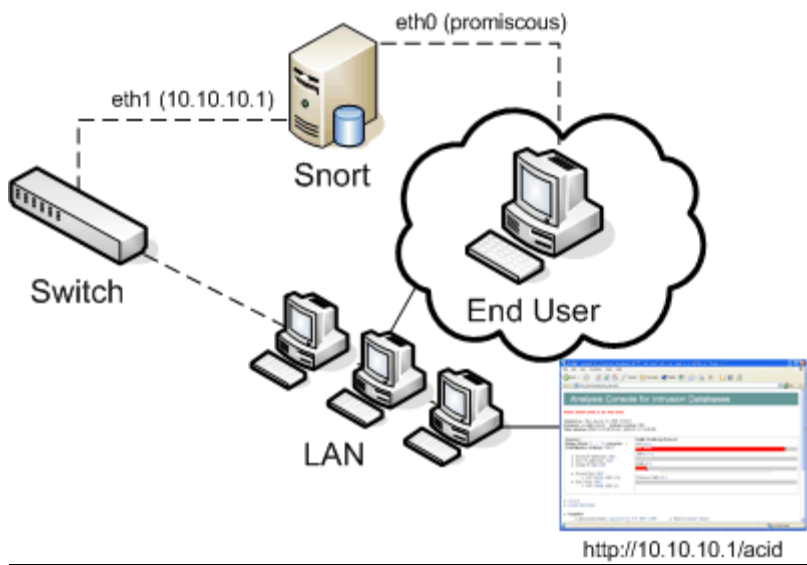


Figure 2

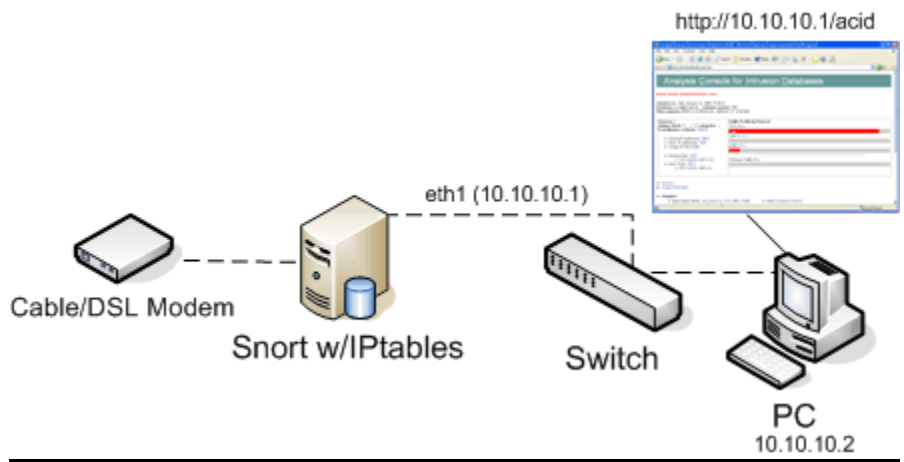


Figure 3

Figure 1

This diagram shows the Snort sensor plugged directly into a switch via eth0 and eth1. The port eth0 is plugged into and can be spanned to mirror another single port or a port on which the Internet access is located (i.e. DSL, T1). Port spanning the LAN's internet access port is a great way to look at the traffic going in/out of the LAN. With this configuration there are many different ways to have snort work for you.

Figure 2

This diagram shows a troubled (i.e. viruses, hacked) PC on a network. The LAN cable is removed, taking it off the LAN to prevent further damage and then the eth0 Snort sensor is plugged into the PC. This is a good method to use to look at any traffic that may be originating from the PC via the ACID interface on another LAN workstation (or on the snort sensor itself).

Figure 3

This is a common and popular way to run snort at home. The diagram shows a Cable/DSL modem directly plugged into the Snort sensor over eth0 (non-promiscuous) with IPtables (firewall) running on it doing NAT. The local PC behind the Snort Firewall is protected with the features of a firewall and an IDS solution on the same box.

Keep in mind these are just a few of many ways to configure snort to work for you. Put a project sheet together on what your goals are, then research how snort can work for you.

Pre-requisites:

- Minor/Newb Linux knowledge. (we will use the VI editor if needed)
- Understanding of TCP/IP configuration
- 2 NIC's (Network Interface Cards)
- Connection to the internet to download the source files
- Coffee, lots of it!

This is an install for a fresh system, the hard disk will be formatted.

Material:

- Mandrake 9.2 (Disc 1,2 and optionally the International Disc)

Misc Information:

Snort website – <http://www.snort.org>

Snort FAQ – <http://www.snort.org/docs/faq.html>

Snort manual – http://www.snort.org/docs/writing_rules/

Snort mailing list – <http://lists.sourceforge.net/lists/listinfo/snort-users>

Pre-Install Checklist:

(use this section to write your notes and configurations prior to the install)

eth1 (Local Area Network)

IP Address	
Netmask	
Gateway	
DNS Servers	
Hostname	

: NOTES :

Acknowledgements:

Where would a document be without proper acknowledgement from those who make it possible? I would like to acknowledge my fiancée, whom has put up with me day and night in my quest for knowledge. Without her support I would be a bachelor.

Next, David Ellis. CCNA, CCSE, MCSE, CCA over at [NightWatch NSS](#), for taking the time to QA this document and verifying that my steps were clear, understandable and got the job done.

Also I would like to thank Patrick Harper, CISSP MCSE over at www.internetsecurityguru.com for letting me use his template for this document. Patrick Harper wrote the [Snort, Apache, PHP, MySQL, ACID on Redhat 9.0 Installation Guide](#). Thanks again.

Don't forget the Snort team over at www.snort.org, without Snort lets just say this document does not exist.

Installing Mandrake 9.2:

The installation of Mandrake 9.2 that we will be doing will be one of the most basic installs you can do that will leave other functionality to the system. It would be a good idea to research "How to harden Linux" documentation. This system can pose a threat to your organization if not properly hardened down. If this system is compromised and root access is obtained (depending on what your monitoring, say an entire switch with port spanning for instance) the user will be able to monitor traffic through the connected segment over eth0 (i.e. packet sniffing).

With that said, let's get to work on this IDS (is the coffee brewing?).

Language:

English (American) – default
Click next

License:

Accept
Click next

Mouse:

PS2\Standard
Click next

Security:

Standard
Click next

Partitioning:

(feel free to customize the partitions you need, but for this document we will stay with the default partition layout)

Erase entire disk
Click next
Confirm all existing data will be lost
Click next

(Mandrake will format the partitions)

Package Selection:

You can install almost anything, as long as you do not install any of the components that we will be installing (listed at the beginning of this document). If this system is going to be used in a Production environment then you should install only the least amount of packages as possible.

For each package you install, you should maintain it by keeping up to date with the Mandrake Update utility. All applications and packages are prone to vulnerabilities.

For this document we will just install the following:
(select only the following)

Internet Station
Configuration
Console Tools
Development
Documentation
LSB
KDE
Click next

If prompted to install any services (i.e. cups, webmin) select NO
Click next

(The Mandrake install will start copying files. Replace the CD's as it asks for them. If it asks for the International CD, click Cancel)

Root Password:

Set a strong root password (i.e. uppercase, lowercase, and alphanumeric) at least 8 characters long and retype it to confirm
Click next

Enter a user:

Create your account. Do not use the same password as the root account. The root account should not be used unless specified. Create a strong password for your user account
Click next

Auto login:

Remove the checkbox from "Do you want to use this function"
Click next

Bootloader Install:

First sector of drive (MBR)
Click next

Summary:

Network – Click configure
Check "Use auto detection"
Check "Expert mode"
Click next
Click LAN Connection – Ethernet card(s) detected
Click next
Click next again
(verify that it found both NIC's)
Select No for "Do you have another one"
Click next

eth0 configuration:

(eth0 will be the interface that monitors the traffic , promiscuously)
Remove checkbox from Automatic IP

Give eth0 a fake IP Address and Netmask (i.e. 192.168.0.1 255.255.255.0)
(after the install we will put eth0 in promiscuous mode)

eth1 configuration:

(eth1 will be the interface that connects to the LAN)

If DHCP:

If your LAN issues DHCP addresses then check off Automatic IP, however, its is recommended to issue a static IP address for ease of management and accessibility. (i.e. creating a static DNS entry for access to the web interface)

If Static:

Give eth1 an IP Address and Netmask that is on the network your connecting to (i.e. 192.168.0.1 255.255.255.0)

Click next

Misc Network information:

Host name: snort.yourdomain.com

Zeroconf host name: snort

DNS servers: Your DNS servers IP address

Gateway: Your LAN Gateways IP address

Gateway device: eth1

Click next

Proxy:

Leave blank

Click next

Configuration is complete; do you want to apply settings?

Select YES

Click next

Click Finish

Summary:

Though this document stays with the defaults, feel free to change any other settings such as Video, resolution, Hardware...etc.

(Don't email me if something doesn't work after the reboot for example, if your monitor resolution is all messed up)

Click next

Install updates:

(using Mandrake update after the install you can get the latest updates. It's recommended to say NO at this point. This document walks you through the install from original files, however it is recommended to keep your system up to date with the latest security patches and updates)

Select No

Click next

Exit Install:

Click reboot

After the reboot:

At the "Welcome to Snort" (xlogin), login as the non-root user we created during the install.

Welcome to the first time wizard:

Click Skip Wizard (feel free to customize)

Welcome to Mandrake Linux:

Clear the check box from "Open this window on startup"
Click close

Congratulations on installing Mandrake 9.2

Before going on. Verify that the NIC eth0 is plugged into the segment that you will be monitoring and NIC eth1 is plugged into the LAN segment. If using DHCP on the eth1 segment, verify you have an IP address using the "ifconfig" command. NIC eth0 will have the fake IP Address we assigned during the install, we will change this to have no IP Address and run in promiscuous mode a little later during the install.

Verify that you can access the internet / ping resources (over eth1) before continuing.

Mandrake Update:

Mandrake Update will keep your system up to date with the latest Security, Bugfixes and Normal updates. It is recommended to run this and update your system at this point.

Click the KDE button (bottom left) > Configuration > Packaging > Mandrake Update (Mandrake Update needs to be run as root; it will prompt you to login as root for this application)

Enter the Root password

Click ok

Click yes to continue with Mandrake Update

Mandrake update will need to download a list of mirrors to get the updates from (it is recommended to make sure your connection out to the LAN/Internet is working).

Click yes

Mandrake Update will display a list of Update mirrors; select the one closest to you

Click ok

Mandrake Update will now display updates for your system

Select Security Updates

Select Bugfix Updates

Select Normal Updates

Check off all the packages displayed or pick and choose what you should update. (It is recommended to update everything)

Click install

(Mandrake may ask for installation media discs, just follow through with the Update until finished)

Click ok when finished

Click quit

Disable Services:

(there are certain services installed by default that we will not need for this snort box)

Click the KDE button > Configuration > Configure your computer

Type the root password

Click ok

Click system on the menu

Click DrakXServices

apmd - Remove the check for "On Boot"

netfs - Remove the check for "On Boot"

portmap - Remove the check for "On Boot"

Click ok

Your Mandrake 9.2 install should now be complete, up to date and ready for the Snort install. Although not required, we will perform a reboot and make sure everything comes up again for the Snort install.

Reboot your system

Downloading the Source installation files

We are now ready to download the source installation files from the respected website. You can either do this from a terminal window or SSH (if you installed this) from another workstation on your LAN.

Create a temp folder on the system to download the files and install from. I will be creating a directory under /root called snortinstall. Using the mkdir command type: mkdir /root/snortinstall. You will need to be logged in as root. At the shell simply type "su -" (without the quotes) and then the root password. This command will give you the root account rights with all of its environment variables.

You can either download all the source files by visiting the following URL's and downloading them to the snortinstall folder, or you can download the snortfiles.sh script from

<http://home.comcast.net/~nduda78/snortfiles.sh>

This script will create the appropriate directory (/root/snortinstall) and download / extract all files to it.

Snort 2.1.0

<http://www.snort.org/dl/snort-2.1.0.tar.gz>

MySQL 4.0.17

<http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.17.tar.gz>

Apache 2.0.48

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

PHP 4.3.4

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

ADODB 3.90

<http://phplens.com/lens/dl/adodb390.tgz>

ACID 0.9.6b23

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

ZLIB 1.2.1

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

JPGGraph 1.14

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

LibPcap 0.8.1

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

Webmin Module 1.121

<http://umn.dl.sourceforge.net/sourceforge/sourceforge/webadmin/webmin-1.121.tar.gz>

Swatch 3.0.8

<http://umn.dl.sourceforge.net/sourceforge/swatch/swatch-3.0.8.tar.gz>

Now that all the files have been downloaded you should verify them. Once you have verified that you have them all we can continue on with the installation. Change into the /root/snortinstall directory.

Installing zlib:

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

Installing LibPcap:

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

Installing MySQL:

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

```
groupadd mysql
useradd -g mysql mysql
```

In /root edit the file **.bash_profile** and add the following line:

```
PATH=$PATH:$HOME/bin:/usr/local/mysql/bin
```

```
tar -zxvf mysql-4.0.17.tar.gz
cd mysql-4.0.17
./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 , edit the file **/etc/ld.so.conf** and add the following lines to it:

```
/usr/local/mysql/lib/mysql
/usr/local/lib
```

save and exit the file then run the command:

```
ldconfig -v
```

Let's test out MySQL now.

```
/usr/local/mysql/bin/mysqld_safe --user=mysql &
(hit enter again to get the command shell back)
```

You should get no errors if the install went properly. Verify this by checking to see if the mysql daemon is running:

```
ps -aux | grep mysql
```

You will see multiple lines of mysql process running similar to the following:

```
root 6814 1637 0 Jan10 vc/1 00:00:00 /bin/sh /usr/local/mysql/bin/mysqld_safe --user=mysql
mysql 6844 0.0 2.5 55892 13060 vc/1 S Jan10 0:00 /usr/local/mysql/libexec/mysqld --
basedir=/usr/local/mysql --datadir=/usr/local/mysql/var --user=mysql --pid-
file=/usr/local/mysql/var/snort.domainname.com.pid --skip-locking --port=3306 --socket=/tmp/mysql.sock
```

Configure MySQL to execute on system startup:

In the mysql source directory run the following command:

```
cp support-files/mysql.server /etc/init.d/mysql
chmod 755 /etc/init.d/mysql
cd /etc/rc3.d
(note: rc3.d is init level 3 startup)
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
cd /etc/rc5.d
(note: rc5.d is init level 5 startup)
ln -s ../init.d/mysql S85mysql
ln -s ../init.d/mysql K85mysql
```

Installation of Apache Web Server w/ PHP:

On the following installation of Apache we will be using “/www” for the installation path. Feel free to modify the directory to your likings.

From the snortinstall directory run the following:

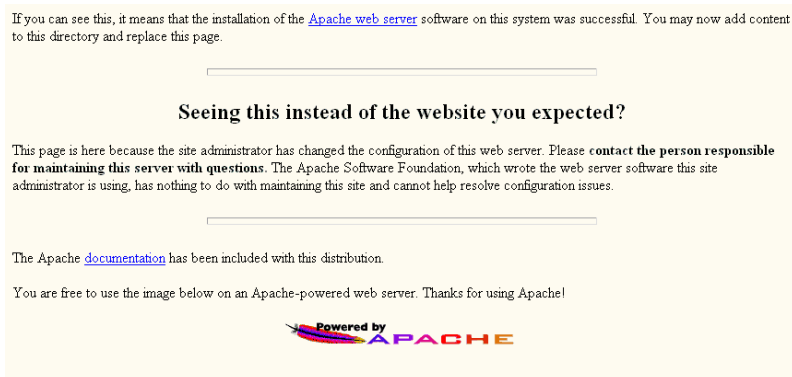
```
tar -zxvf httpd-2.0.48.tar.gz
cd httpd-2.0.48
./configure --prefix=/www --enable-so
make
make install
```

Test the install of apache by trying to start the daemon

```
/www/bin/apachectl start
```

Open a web browser and navigate to the Snort machines IP address (i.e. <http://10.10.10.1>). You may get an error about the hostname, don't worry about that.

If apache is running properly your browser will as followed:



Stop the apache server:

```
/www/bin/apachectl stop
```

Installation of PHP:

```
cd..  
tar -zxvf 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 (all on one line)  
make  
make install
```

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

Now we need to make some changes in the Apache web server configuration file to include PHP scripting to parse.

Using your editor of choice, VI is great; pico is easier, edit /www/conf/httpd.conf

Add the following lines: (search the httpd.conf file for the proper sections for these lines. Using VI type "/LoadModule" and it will bring the cursor to the LoadModule section.)

```
LoadModule php4_module modules/libphp4.so  
AddType application/x-httpd-php .php  
DirectoryIndex index.php index.html
```

Apache w/PHP has been successfully installed.

Configure Apache to execute on system startup:

```
cp /www/bin/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
```

Lets test Apache again and see if its is parsing PHP documents now. Create a file in /www/htdocs (htdocs is the directory that holds the web files that are being served) called phpinfo.php and add the following line:

```
<?php phpinfo(); ?>
```

Exit and save the file. Next start the apache daemon.

```
/etc/rc5.d/S85httpd start
```

Open a web browser and navigate to the IP address of the system calling the php file (i.e. http://10.10.10.1/phpinfo.php)

You should see the following webpage:

PHP Version 4.3.4



System	Linux snort. 2.4.22-10mdk #1 Thu Sep 18 12:30:58 CEST 2003 i686
Build Date	Jan 12 2004 03:25:02
Configure Command	'./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'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/php/php.ini
PHP API	20020918
PHP Extension	20020429
Zend Extension	20021010
Debug Build	no
Thread Safety	disabled
Registered PHP Streams	php, http, ftp, compress.zlib

Congratulations on installing Apache w/PHP

Installation of Snort:

Let's start by putting eth0 in promiscuous mode. Edit the file: /etc/sysconfig/network-scripts/ifcfg-eth0

Change the file to display the following:

```
DEVICE=eth0
BOOTPROTO=
ONBOOT=yes
```

Save and exit the file. Bring the eth0 interface down (disable) then back up (enable):

```
ifdown eth0
ifup eth0
```

Next run ifconfig to see the Ethernet configuration:

```
eth0   Link encap:Ethernet HWaddr 00:50:8B:AC:06:18
       UP BROADCAST RUNNING MULTICAST  MTU: 1500  Metric: 1
       RX packets:290547660 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen: 100
       RX bytes:3060633216 (2918.8 Mb) TX bytes:0 (0.0 b)
       Interrupt:16 Base address:0x8000

eth1   Link encap:Ethernet HWaddr 00:08:02:BC:06:B7
       inet addr:10.1.0.60 Bcast:10.1.0.255 Mask:255.255.0.0
       UP BROADCAST RUNNING MULTICAST  MTU: 1500  Metric: 1
       RX packets:11618790 errors:0 dropped:0 overruns:0 frame:0
       TX packets:1084781 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen: 100
       RX bytes:1007600167 (960.9 Mb) TX bytes:212941214 (203.0 Mb)
       Interrupt:20 Base address:0xa000
```

Notice eth0 no longer has an IP Address , but is active. Eth0 is now in promiscuous mode.

Next we will add the group and user that snort will be using.

```
groupadd snort
useradd -g snort snort
```

Next, create the directory that will hold the rules and conf file and the log directory.

```
mkdir /etc/snort
mkdir /var/log/snort
```

Now, lets untar / install snort

```
cd /root/snortinstall/
tar -zxvf snort-2.1.0.tar.gz
./configure --with-mysql=/usr/local/mysql
make
make install
```

Installing the default rules and conf file:

```
cd rules
cp * /etc/snort
cd ../etc
cp snort.conf /etc/snort
cp threshold.conf /etc/snort
cp *.config /etc/snort
cp *.map /etc/snort
```

Now we need to modify the snort.conf file. This file is key to making sure everything runs properly. If snort isn't running properly, most likely it is a configuration issue within this file.

Edit /etc/snort/snort.conf and make the following changes

```
var HOME_NET 10.10.10.0/24 (change this to your internal network range)

var RULE_PATH /etc/snort
```

Now we need to tell snort how to log.

Log to MySQL:

Locate the output section of the configuration file (around line 450) and add the following on one line:

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

Log to SYSLOG:

Logging to syslog is not required if you don't plan on using SWATCH later in the installation document. The problem with regular logging is that the alerts are not all on one line which makes SWATCH logging rather ineffective.

Add the following line just below the MySQL logging line:

```
output alert_syslog: LOG_AUTH LOG_ALERT
```

Misc configuration:

There is plenty more to configure within this file but beyond the scope of this document. Familiarize yourself with the snort.conf file. Once you're comfortable within it you can tweak it to be more efficient in logging without creating false positives. Configuring variables for different servers and services is key to setting up and having an effective snort sensor. Some of the other key options to configure would be:

```
var SMTP_SERVERS
var DNS_SERVERS
var HTTP_SERVERS
var SQL_SERVERS
var SNMP_SERVERS
```

If your company has a "policy":

```
var AIM_SERVERS
var IRC_SERVERS
var MSN_SERVERS
```

Defining variables will help keep your snort sensor running accurately, and with less false positives.

Configure Snort to execute on system startup:

From the snort source install directory:

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

We need to edit /etc/init.d/snort now and change the following configuration lines:

```
CONFIG=/etc/snort/snort.conf
SNORT_GID=snort
```

Save and exit /etc/init.d/snort

```
chmod 755 /etc/init.d/snort
```

```
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
```

Creating the Snort MySQL database:

Lets start by entering into MySQL, run:

```
/usr/local/mysql/bin/mysql
```

At the mysql> prompt type the following: Note: pick your own password and replace it where it says new_password

```
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
```

Now we need to insert the snort database into MySQL. Change into the snort source directory /root/snortinstall/snort-2.1.0 and run the following command:

If asked for a password, enter the one you defined when configuring the snort database in mysql.

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

Now install the Snort DB tables into the database. Enter the following:

```
zcat contrib/snortdb-extra.gz | /usr/local/mysql/bin/mysql -p snort
```

Now to verify the database.

```
/usr/local/mysql/bin/mysql -p
>Enter Password:
mysql> SHOW DATABASES;
```

```
+-----+
| 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)
```

```
mysql> exit
>Bye
```

Edit the snort.conf file located in /etc/snort
Locate the line used to log to MySQL and change the password from "new_password" to the one you created in the MySQL DB creation in the previous step.

Installation of JpGraph:

Change directories to /root/snortinstall and run the following:

```
cp jpgraph-1.14.tar.gz /www/htdocs
cd /www/htdocs
tar -zxvf jpgraph-1.14.tar.gz
rm -rf jpgraph-1.14.tar.gz
cd jpgraph-1.14
rm -rf README
rm -rf QPL.txt
```

Installation of ADODB:

Change directories to /root/snortinstall and run the following:

```
cp adodb390.tgz /www/htdocs
cd /www/htdocs
tar -zxvf adodb390.tgz
rm -rf adodb390.tgz
```

Installing ACID:

Change directories to /root/snortinstall and run the following:

```
cp acid-0.9.6b23.tar.gz /www/htdocs
cd /www/htdocs
tar -zxvf acid-0.9.6b23.tar.gz
rm -rf acid-0.9.6b23.tar.gz
```

ACID Configuration:

Change directories to /www/htdocs/acid and edit the file acid_conf.php

Change it to the following (using the password you specified):

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

/* The type of underlying alert database
 *
 * MySQL      : "mysql"
 * PostgreSQL : "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";

Further down

/* Path to the graphing library
 * (Note: DO NOT include a trailing backslash after the directory) */ $ChartLib_path =
"/www/htdocs/jpgraph-1.14/src";

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

Now let's start up Apache "/etc/rc5.d/S85httpd start" then open a web browser and navigate to the following link:

http://yoursnortmachine/acid/acid_main.php

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 "Setup Page". This will create the DB Tables for ACID

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

[Back]

Operation	Description	Status
ACID tables	Adds tables to extend the Snort DB to support the ACID functionality	<input type="button" value="Create ACID AG"/>
Search Indexes	(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)

Click the button "Create ACID AG"

Now close the browser, open a new browser and navigate to:

<http://yoursnortmachine/acid/>

Analysis Console for Intrusion Databases

Added 0 alert(s) to the Alert cache

Queried on : Mon October 06, 2003 15:49:15
Database: snort@localhost (schema version: 106)
Time window: no alerts detected

Sensors: 0 Unique Alerts: 0 (0 categories) Total Number of Alerts: 0 <ul style="list-style-type: none">• Source IP addresses: 0• Dest. IP addresses: 0• Unique IP links 0 • Source Ports: 0<ul style="list-style-type: none">◦ TCP (0) UDP (0)• Dest. Ports: 0<ul style="list-style-type: none">◦ TCP (0) UDP (0)	Traffic Profile by Protocol TCP (0%) <hr/> UDP (0%) <hr/> ICMP (0%) <hr/> Portscan Traffic (0%) <hr/>
---	---

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

Securing the ACID directory:

For security purposes the ACID directory should be secured to only allow users that you want to view the ACID console. This step is recommended if using Snort on a Production LAN.

```
mkdir /www/passwords
```

(the username we will be using is acid, feel free to use whatever you want)

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

Enter the password for the user. This username and password is what will be required when viewing the ACID console.

Now we need to edit our Apache config file to secure the ACID directory. Edit the file httpd.conf in the /www/conf directory. Look for the section that start with </Directory> and then add the following replacing "user acid" with whichever user you choose. Multiple users can be added by spaces:

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

Now restart the Apache daemon again

```
"/etc/rc5.d/S85httpd start"
```

 and navigate to the following webpage:

<http://yoursnortmachine/acid>

You should be prompted for a username and password. Enter the username and password we created in the last step. You should now be in the ACID console.

Start Snort now by executing the following:

```
/etc/rc5.d/S99snort
>Starting Intrusion Database System: SNORT
> Snort is up and running!
```

Verify the snort daemon is running:

```
ps -aux | grep snort
```

Congratulations on your installation of Snort, Apache, PHP, MySQL, JGraph, Zlib, Libpcap and ACID. Now let's get into actively monitoring the snort sensor and the Webmin module.

Installing the Webmin Module:

Navigate back to /root/snortinstall and run the following:

```
tar -zxvf webmin-1.121.tar.gz
cd webmin-1.121
./setup.sh
"Config file directory [/etc/webmin]:"
Press enter
" Log file directory [/var/webmin]:"
Press enter
"Full path to perl (default /usr/bin/perl):"
Press enter
```

For "Web server port (default 10000):" you can either hit enter to use the default port of 10000 or choose your own port to listen on. Port 10000 is widely known for Webmin (isn't that obvious). It's recommended with Webmin to choose a different port than 10000. For this document however we will stay with the default (this can be changed at a later time). Press Enter to accept the default port.

"Login name (default admin):"
Press Enter to user admin or create your own user

"Login password:"
Type in a password for the user you just created

"Password again:"
Type it in again to verify you spelt it correctly

"Use SSL (y/n):"
Press Y then enter

"Start Webmin at boot time (y/n):"
Press Y then enter

```
*****
Webmin has been installed and started successfully. Use your web
browser to go to
```

```
https://yoursnortmachine:10000/
```

and login with the name and password you entered previously.

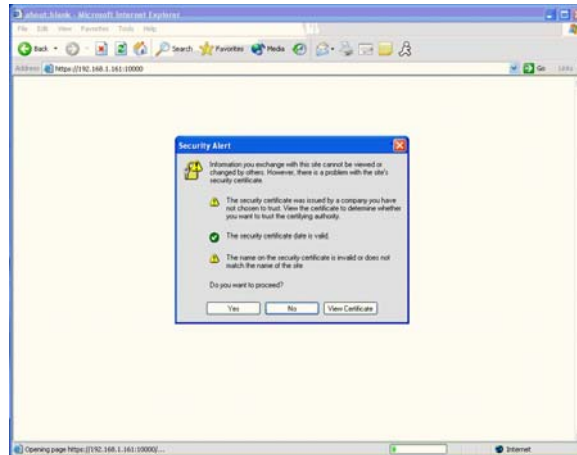
Because Webmin uses SSL for encryption only, the certificate

it uses is not signed by one of the recognized CAs such as Verisign. When you first connect to the Webmin server, your browser will ask you if you want to accept the certificate presented, as it does not recognize the CA. Say yes.

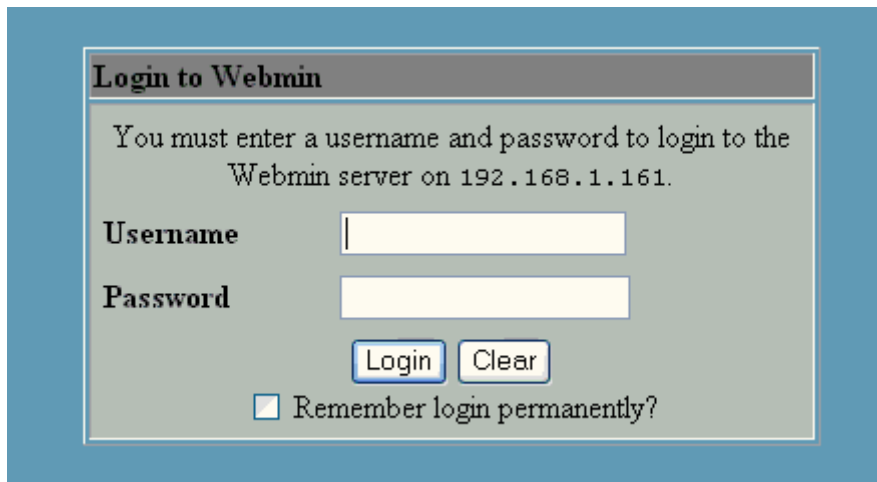
Opening Webmin:

Open a web browser and navigate to <http://yoursnortmachine:10000>

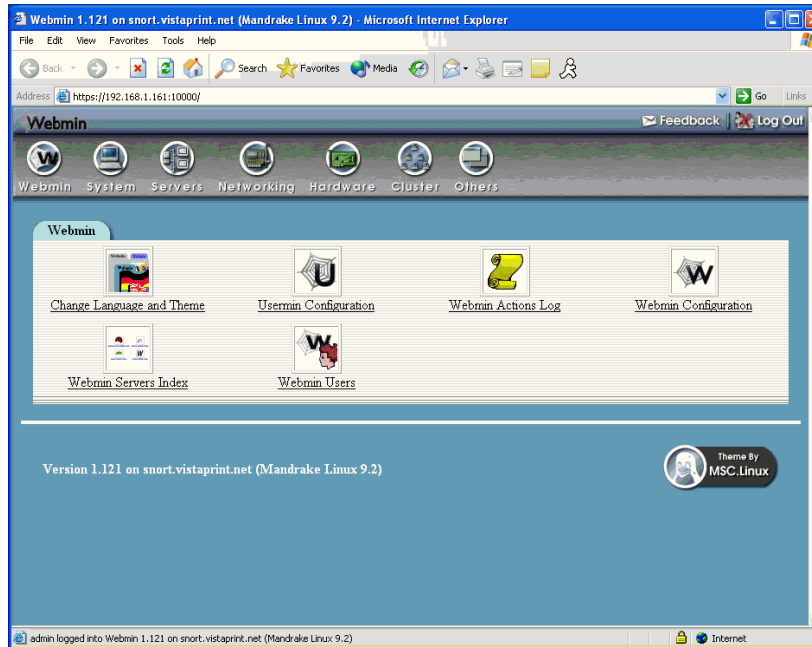
Click Yes to accept the SSL certificate



Enter the username and password for Webmin that you created during the install then press Login



Webmin is now installed and running over SSL. Webmin can be used for many different administration tasks.



Installing the Webmin module for Snort:

Login to Webmin and on the Webmin tab click on the Webmin Configuration icon

Click on Webmin Modules

Select "From ftp or http URL"

Enter <http://www.msbnetworks.com/snort/download/snort-1.1.wbm>

Click Install Module

The following will be displayed:

```
-----  
Downloading http://www.msbnetworks.com/snort/download/snort-1.1.wbm ..  
Downloading http://msbnetworks.net/snort/download/snort-1.1.wbm (102400 bytes) ..  
  Received 1024 bytes (1 %)  
  Received 10240 bytes (10 %)  
  Received 20480 bytes (20 %)  
  Received 30720 bytes (30 %)  
  Received 40960 bytes (40 %)  
  Received 51200 bytes (50 %)  
  Received 61440 bytes (60 %)  
  Received 71680 bytes (70 %)  
  Received 81920 bytes (80 %)  
  Received 92160 bytes (90 %)  
  Received 102400 bytes (100 %)  
.. Download complete.
```

The following modules have been successfully installed and added to your access control list :

Snort IDS Admin in /root/snortinstall/webmin-1.121/snort (180 kB) under category Servers

```
-----
```

Click on the Servers icon in Webmin

You should now have the Snort Module for Webmin installed:



Configuring Snort to work in Webmin:

Click on the Snort IDS Admin button

Type the following into the initial configuration:

Full path to Snort executable (with options)

`/usr/local/bin/snort -c /etc/snort/snort.conf -i eth0 -g snort -D`

Full path to Snort configuration file

`/etc/snort/snort.conf`

Full path to Snort rule files directory

`/etc/snort`

Full path to Snort PID file

`/var/run/snort_eth0.pid`

Command to start Snort (optional)

Leave this blank

URL to ACID (optional)

`http://yournortmachine/acid`

Click Save

The following step is required if you plan on modifying rules/signatures using the Webmin console instead of physically editing the rules file.

If you click on a rule to modify it, you may get a message like the following:



Webmin out of the box doesn't read the snort variable \$RULES_PATH correctly, we need to modify the snort.conf file and change how the rules are listed. You can edit the snort.conf file from the Webmin module.

Edit `/etc/snort/snort.conf`

Scroll to the bottom on the conf file to the rules. They should look like this:

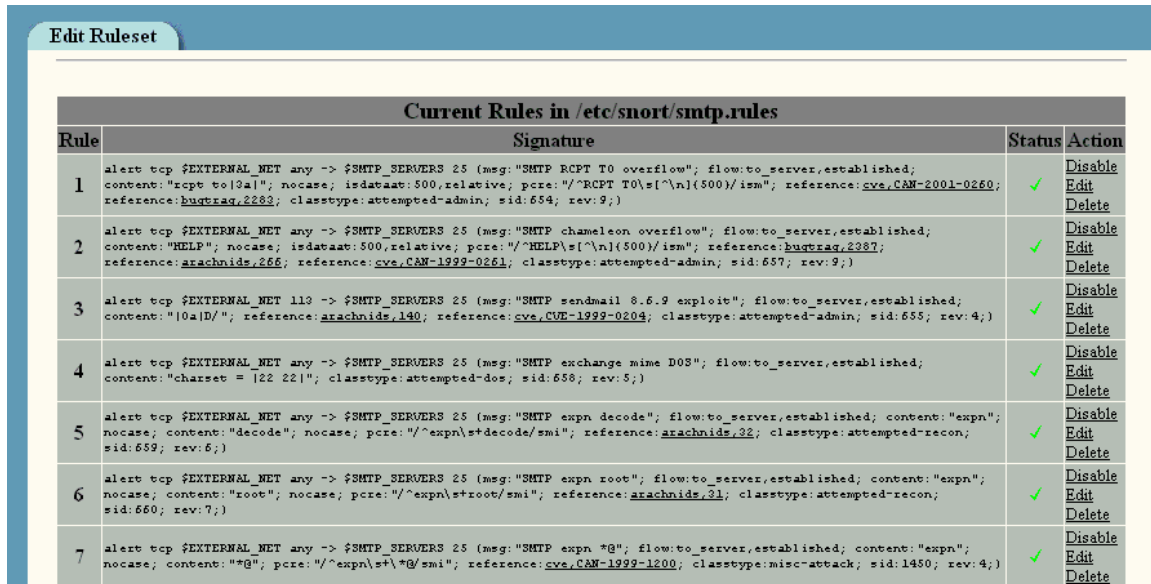
```
include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
...etc
```

Change each line with a rule to look like the following:

```
include local.rules
include bad-traffic.rules
include exploit.rules
include scan.rules
include finger.rules
include ftp.rules
...etc
```

Save and exit the file.

Log out and back into the Webmin interface and click on a rule to edit, you should be able to modify, add and remove rules.



Current Rules in /etc/snort/smtp.rules			
Rule	Signature	Status	Action
1	alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"SMTP RCPT TO overflow"; flow:to_server,established; content:"rcpt to 0a "; nocase; isdataat:500,relative; pcre:"/^RCPT TO\s{0,1000}/ism"; reference:cve,CAN-2001-0260; reference:bugtraq,2282; classtype:attempted-admin; sid:654; rev:9;)	✓	Disable Edit Delete
2	alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"SMTP chameleon overflow"; flow:to_server,established; content:"HELP"; nocase; isdataat:500,relative; pcre:"/^HELP\s{0,1000}/ism"; reference:bugtraq,2387; reference:arachnids,266; reference:cve,CAN-1999-0261; classtype:attempted-admin; sid:657; rev:9;)	✓	Disable Edit Delete
3	alert tcp \$EXTERNAL_NET 113 -> \$SMTP_SERVERS 25 (msg:"SMTP sendmail 8.6.9 exploit"; flow:to_server,established; content:" 0a D/"; reference:arachnids,140; reference:cve,CVE-1999-0204; classtype:attempted-admin; sid:655; rev:4;)	✓	Disable Edit Delete
4	alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"SMTP exchange mime DOS"; flow:to_server,established; content:"charset = 22 22 "; classtype:attempted-dos; sid:658; rev:5;)	✓	Disable Edit Delete
5	alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"SMTP expn decode"; flow:to_server,established; content:"expn"; nocase; content:"decode"; nocase; pcre:"/^expn\s+decode/smi"; reference:arachnids,32; classtype:attempted-recon; sid:659; rev:6;)	✓	Disable Edit Delete
6	alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"SMTP expn root"; flow:to_server,established; content:"expn"; nocase; content:"root"; nocase; pcre:"/^expn\s+root/smi"; reference:arachnids,31; classtype:attempted-recon; sid:660; rev:7;)	✓	Disable Edit Delete
7	alert tcp \$EXTERNAL_NET any -> \$SMTP_SERVERS 25 (msg:"SMTP expn *@"; flow:to_server,established; content:"expn"; nocase; content:"*@"; pcre:"/^expn\s+*/smi"; reference:cve,CAN-1999-1200; classtype:misc-attack; sid:1450; rev:4;)	✓	Disable Edit Delete

Congratulations, the Snort Webmin module has been installed. There are numerous things you can do from this console, make sure you find time to explore it.

Installation of Swatch:

Swatch requires that you have a mail daemon installed such as Sendmail or Postfix. The install we did should have installed postfix on this system. If one is not installed, you can use the Mandrake Install Software utility or do it manually by source. I recommend postfix for this purpose.

Verify that you can send an email out from this system by doing the following example:

```
/bin/uname -a | /bin/mail -s "Test Email" your@emailaddress.com
```

This will email the results of uname to the specified email address with the subject of Test Email. If you got this email then the mail daemon is running on the snort host. If you do not get the email you may have to make changes to your mail daemon and try again.

Swatch also requires the CPAN modules:

```
Date::Calc  
Date::Parse  
File::Tail  
Time::HiRes
```

These like the mail daemon can be installed using the Mandrake Install Utility or using the script I wrote located at http://www.secured-systems.com/scripts/swatch_span.sh

Once your mail daemon is running install Swatch. Navigate to the /root/snortinstall directory.

```
tar -zxvf swatch-3.0.8.tar.gz  
cd swatch-3.0.8  
perl Makefile.PL  
make  
make test  
make install
```

Swatch is now installed. When Swatch is executed it runs against a configuration file (that we will make in the next step). Swatch actively monitors the system logs including syslog for any events that we specify in the configuration file. When a match is found, swatch can do the following:

- Echo the match to the terminal
- Email the alert
- Execute

The echo alert function of swatch simply echo's the matched alert to the terminal it is running on.

The email alert function of swatch is limited but effective. It will simply send an email to the specified email address with the matched alert as the body.

The execute alert can execute an external function, such as a script. Being able to harness the power of executing scripts with carrying the matched alert variable over is extremely powerful.

I will provide examples of all three alerts.

Creating the Swatch Configuration file:

The swatch configuration file will hold a section for each alert you want. We will specify in the alert what to look for in the logs and then how to act on it.

Create and edit a file called swatch.conf in /etc/snort and add the following text:

```
# Alert on SSH connections  
watchfor / snort: /, / ssh /  
echo  
mail=your@emailaddress.com,subject=SnortAlert:SSH_Activity
```

Save and exit this file. This example will wait for an alert to appear with "snort:" and "ssh" in the syntax. If this rule matches, it will "echo" the alert to the terminal and then email the alert to your email address with the subject "SnortAlert:SSH_Activity"

Now that we have made the configuration file, its time to start swatch up using it. From the command line enter the following:

```
/usr/bin/swatch --config-file=/etc/snort/swatch.conf
```

The following will display:

```
*** swatch version 3.0.8 (pid:9800) started at Wed Jan 14 10:56:52 EST 2004
```

Swatch will just sit and wait for an alert, if you want to run swatch in the background run the following command:

```
/usr/bin/swatch --config-file=/etc/snort/swatch.conf &
```

Now try to generate some SSH traffic that the segment eth0 is plugged into will see. If successful you will get the alert echoed to the terminal and an email:

```
Jan 14 11:21:16 localhost snort: [1:1000009:1] SSH Activity detected [Classification: Misc activity] [Priority: 3]: {TCP} x.x.x.x:3135 -> x.x.x.x:22
```

To have Swatch execute an external program such as a script for the alert, modify the file to:

```
# Alert on SSH connections
  watchfor / snort: /, / ssh /
  echo
  exec /path/to/script/script.sh $0
```

This will exec the script "script.sh" passing the alert syntax over as the variable \$0 (keep in mind that in the script the variable is no longer \$0 it will be \$*)

With Swatch you can get alerted on whatever you want, it doesn't just have to be snort content. As an example, I use swatch to read syslog messages of VPN connections established that come down from my VPN device. I then awk apart the alert and construct an email that notifies me of when users connect to the VPN. I also have the script to port scans against the vpn connection, pen-testing...etc and it all gets emailed to me every time someone connects to the VPN. Swatch is a great alerting tool.

That concludes this installation document. If you have any questions or feedback, please let me know so I can improve on it @ nduda@secured-systems.com. I am also available for Bash shell scripting if you need help with writing scripts to use with swatch.