Snort Install Manual

Snort, Apache, SSL, PHP, MySQL, and BASE Install on Fedora Core 3

By Patrick Harper | CISSP, RHCT, MCSE
with contributions and editing by Nick Oliver | CNE

http://www.InternetSecurityGuru.com

BASE – Basic Analysis and Security Engine

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). Also, PLEASE READ THIS ENTIRE DOCUMENT.

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. My wife Kris, Nick Oliver (He downloaded and used the first document I wrote and volunteered to do test installs and proof the spelling and punctuation for the following documents. He has become quite proficient with Linux and Snort and is a valued member of the ISG team and contributor to this and other documentation. I would also like to thank the people from the snort-users list and ntsug-users list that helped. Also I would like to thank Marty and the Snort team for their great work. Thanks for staying true to open source.

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 use the most up to date version I will do my best to keep it updated.

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
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 (Thanks Erek)

RedHat Support documents for Fedora –
http://fedora.redhat.com/docs/release-notes/

Websites to visit:
http://www.Snort.org
http://secureideas.sourceforge.net/
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**)

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 whenever I can.

Installing Fedora Core 3:

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 be ideal as a 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

Upgrade Exam:
If this comes up choose Install Fedora Core

Install Type:
Choose custom

Disk Partitioning:
Choose to automatically partition the hard drive. - then
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

When the warning dialog comes up, choose Yes.

Accept the default layout. Most of the disk will be /

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
Set a gateway and the 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:
Choose "enable firewall"
Select remote login (SSH) and Web Server (HHTP, HTTPS)

For the SELinux option, move to Disabled.

Additional Language:
Choose only US English

Time Setup:
Choose the closest city within your time zone (for central choose Chicago)

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

- VNC Server

Gnome Desktop Environment – Accept the default (checked)

KDE Desktop Environment - Accept the default (unchecked)

XFCE - Accept the default (unchecked)

Applications:
Editors – Choose your favorites, however, VIM-Enhanced is suggested and is part of the base install. Nano is also installed, it is easy to use if you are a Linux newbie.

Engineering and Scientific – Accept the default (unchecked)

Graphical Internet – Checked by default, click on details and uncheck the following

- Gnomemeeting
- Xchat
- Gaim
- Evolution
- Evolution-webcal

Text based internet – checked by default, click on details and check the following

- lynx
- ncftp (optional – this is an enhanced ftp client)

Uncheck the following

- mutt
- slm

- cadaver
- fetchmail

Office/Productivity – Only gpdf should be checked. Uncheck everything else.

Sound and Video – None of this is needed

Authoring and Publishing – None of this is needed

Graphics – make sure it is unchecked

Games and Entertainment – None of this is needed

Server Section:
Server configuration tools
- Check and leave at the default

Web Server – ONLY the following should be checked
- Crypto-Utils
- dstcache
- Mod_auth_mysql
- Mod_perl
- Mod_ssl
- Php
- Php_mysql
- Webalizer (if you want to be able to view your logs graphically)

Mail Server – none

Windows File Server – None

DNS server – None

FTP server – None

Postgresql Database - None

MySQL Database– Check only the following
- MyODBC
- Mod_auth_mysql
- Mysql-devel
- Mysql-server
- Perl-DBD-MySQL
- Php-mysql

News server – none

Network Servers – None

Legacy network servers – None

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

- Expect
- Gcc-objc

X Software Development – check this one and accept the default under optional packages.

Gnome Software Development – Leave this unchecked

KDE Software Development – Leave this unchecked

XFCE Software Development – Leave unchecked

Legacy Development – Leave unchecked

System:
Administration – check and accept default

System Tools – check this one and check the following in addition to what is checked:

- Ethereal gnome
- Nmap frontend

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

Miscellaneous:
Choose nothing from this entire section

Hit next, then next again. It will tell you that you will need 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, but remember, 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 3 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. Otherwise it will not be your system for long

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. (for help with sudo visit google.com)

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. Then click on the RedHat on the top

left of your desktop. Select System Settings - Server Settings - Services. This will bring up the list of services that start when the system boots up. Disable the following, then hit save. apmd, cups, isdn, netfs, nfslock, pcmcia, portmap

Update your system

Open up a terminal window to do this. Click on the Red Hat in the top left corner of your desktop. Select System Tools – Terminal. (You can also put this icon on your toolbar by right clicking on it and selecting that option.)

We will be using Yum to keep the system up to date. First we will have to import the GPG key. In the terminal window type:

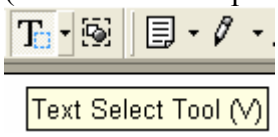
rpm --import /usr/share/rhn/RPM-GPG-KEY-fedora

Then type "yum -y update" and it will check what you need and install it.

(Type "chkconfig yum on" to turn on nightly updates, this is a suggested step) you will need to reboot after this because a new kernel will have been installed during the yum update.

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



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.

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

Save the file and type "service sshd restart". ssh will restart, enacting these changes. (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)

Turn on and set to start the services you will need

chkconfig httpd on
chkconfig mysqld on
service httpd start
service mysqld start

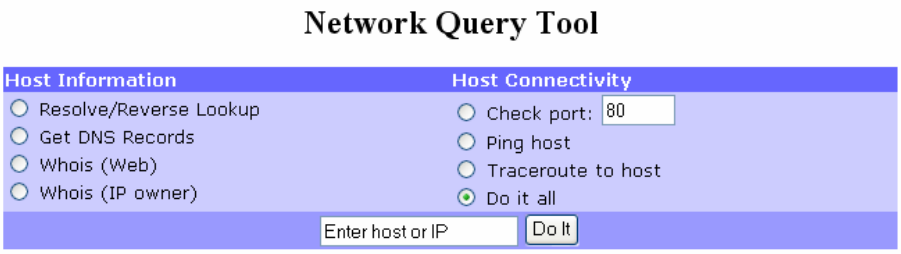
Testing Apache

To test the Apache and PHP, create a file called test.php in the /var/www/html directory. Place the following line in the file:

<?php phpinfo(); ?>

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.

Install the Network Query Tool, using http://shat.net/php/nqt/nqt.php.txt. Copy the text into a file called index.php and place it in the /var/www/html directory, it will look like the following:



Download all the needed files:

Place all the downloaded files into a single 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. From the Terminal window type:

cd /root
mkdir snortinstall

Remember, you can always check where you are currently by typing "pwd" in the terminal window. 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.

Download Snort and PCRE

You can do this from a browser window or use wget from the terminal. From inside of the /root/snortinstall directory, type:

wget http://www.snort.org/dl/snort-2.3.0.tar.gz

When that is downloaded, type:

wget http://umn.dl.sourceforge.net/sourceforge/pcre/pcre-5.0.tar.gz

Install PCRE

tar –xvzf pcre-5.0.tar.gz
cd pcre-5.0
./configure
make
make install

Installing and setting up Snort and the Snort rules:

tar -xvzf snort-2.3.0.tar.gz
cd snort-2.3.0
./configure --with-mysql
make
make install

groupadd snort
useradd -g snort snort

mkdir /etc/snort
mkdir /etc/snort/rules
mkdir /var/log/snort

Installing the rules and conf file:
(From the Snort installation directory)

cd rules
cp * /etc/snort/rules
cd ../etc
cp * /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, use CIDR. If you do not know CIDR then go to http://www.oav.net/mirrors/cidr.html)
var EXTERNAL_NET !$HOME_NET (this means everything that is not your home net is external to your network)

change "var RULE_PATH ../rules" to "var RULE_PATH /etc/snort/rules"

Now tell snort to log to MySQL
Go down to the output section and uncomment the following line. Change it to be like the following except the password. Remember what you make it because you will need it later when you set up the snort user in mysql.

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

Make snort start with the system

Add a line to /etc/rc.local that reads like the following text.
"/usr/local/bin/snort -c /etc/snort/snort.conf -i eth0 -g snort"

Snort will now start automatically for you when you start the system

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)
('password' is whatever password you want to give it, just remember what you assign. For the snort user use what you put in the output section of the snort.conf in the section above)

```
mysql
mysql>  SET PASSWORD FOR root@localhost=PASSWORD('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('password_from_snort.conf');
```

```
>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
```

Execute the following commands to create the tables

mysql -u root -p < ~/snortinstall/snort-2.3.0/schemas/create_mysql snort
Enter password: the mysql root password

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

```
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
| icmphdr
| iphdr
| opt
| reference
| reference_system
| schema
| sensor
| sig_class
| sig_reference
| signature
```

```
| tcphdr
| udphdr
+------------------+
16 rows in set (0.00 sec)
exit;
```

BASE Install

Go to your snort download directory

Type “yum install php-gd” this will install gd for proper graphing in BASE

It will ask you the following, choose Y

```
Transaction Listing:
  Install: php-gd.i386 0:4.3.10-3.2
Is this ok [y/N]: y
```

cd /root/snortinstall

Download ADODB
wget http://umn.dl.sourceforge.net/sourceforge/adodb/adodb460.tgz

Download JPGraph
wget http://www.aditus.nu/jpgraph/downloads/jpgraph-1.16.tar.gz

Download BASE
wget http://umn.dl.sourceforge.net/sourceforge/secureideas/base-1.0.1.tar.gz

Install JPGraph:

Go back to your downloads directory
cp jpgraph-1.16.tar.gz /var/www/html
cd /var/www/html
tar –xvzf jpgraph-1.16.tar.gz
rm –rf jpgraph-1.16.tar.gz
cd jpgraph-1.16
rm -rf README
rm -rf QPL.txt

Installing ADODB:

Go back to your download directory
cp adodb460.tgz /var/www/html/
cd /var/www/html
tar -xvzf adodb460.tgz

rm –rf adodb460.tgz

Installing and configuring BASE:

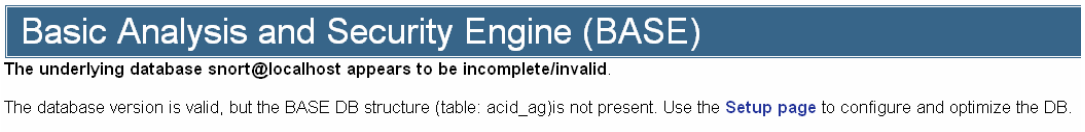
Go back to your download directory
cp base-1.0.1.tar.gz /var/www/html/
cd /var/www/html
tar –xvzf base-1.0.1.tar.gz
rm –rf base-1.0.1.tar.gz

cd /var/www/html/base/
cp base_conf.php.dist base_conf.php

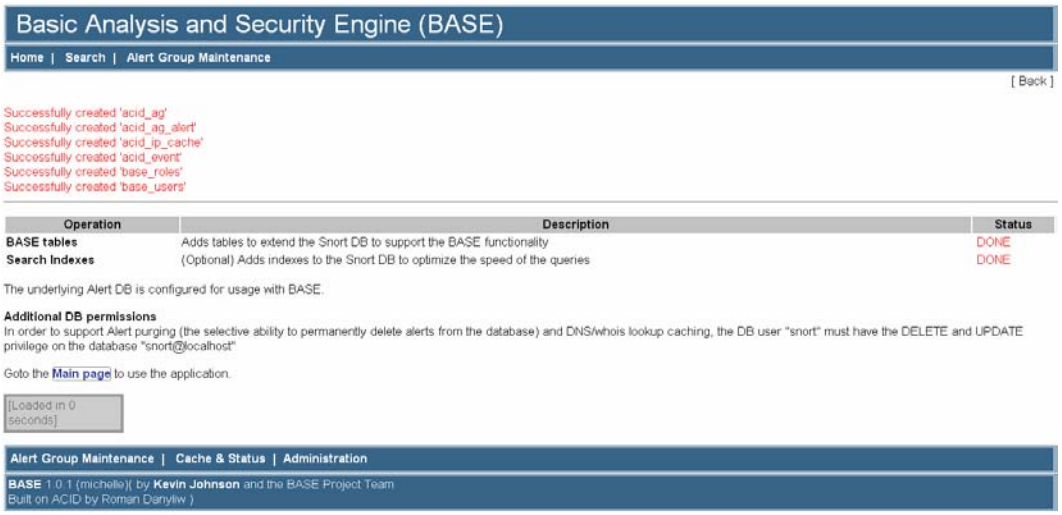
edit the "base_conf.php" file and insert the following perimeters

```
$BASE_urlpath = "/base";

$DBlib_path = "/var/www/html/adodb";
$DBtype = "mysql";

$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "snort";
$alert_password = "password_from_snort_conf";

$archive_dbname   = "snort";
$archive_host     = "localhost";
$archive_port     = "";
$archive_user     = "snort";
$archive_password = " password_from_snort_conf ";

$ChartLib_path = "/var/www/html/jpgraph-1.16/src";
```

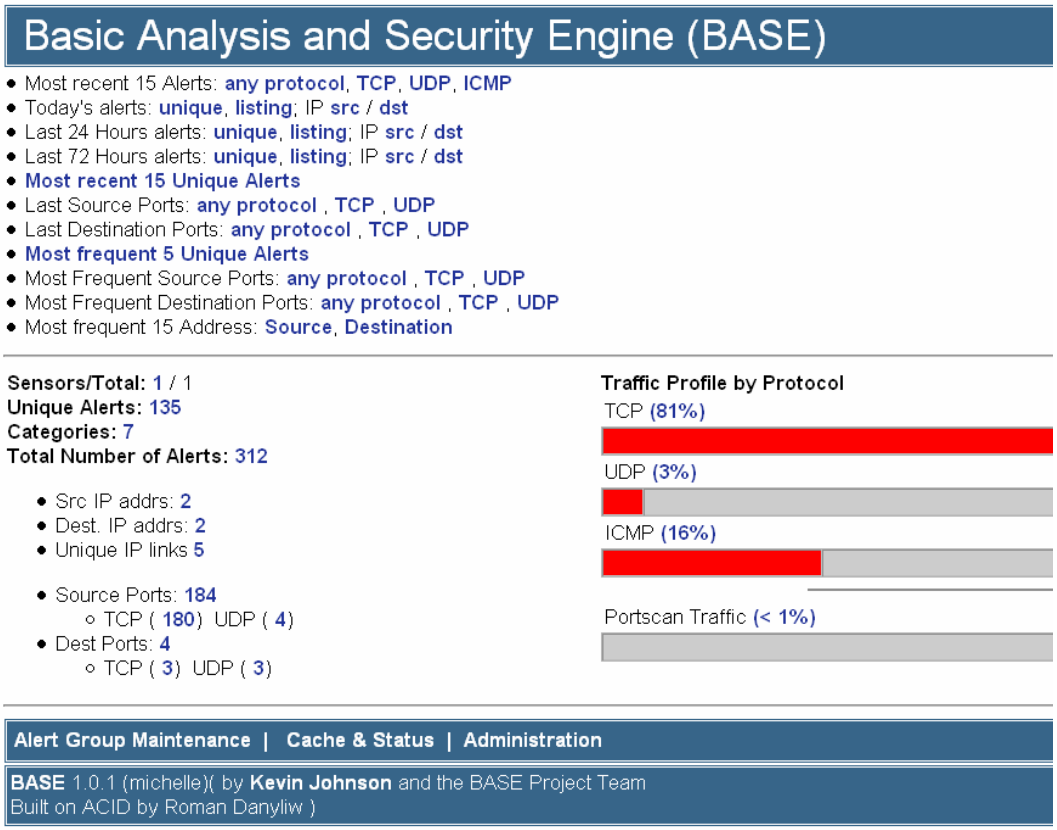
Open a browser window. If the browser is on the localhost, then enter localhost/base. If on another machine, open your browser, enter the ip address of the sensor machine ie, http://ip_address/base



Click the "setup page" link, then on the resulting page, click on the setup AG button. Then you will get the following page.



Click the main page on the bottom and you should see the BASE page



Securing the BASE directory:

mkdir /var/www/passwords

/usr/bin/htpasswd -c /var/www/passwords/passwords base

(base 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 base page

Edit the httpd.conf (/etc/httpd/conf) , I put it under the section that has:

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

These are the lines to add to password protect the BASE console:

```
<Directory "/var/www/html/base">
    AuthType Basic
    AuthName "SnortIDS"
    AuthUserFile /var/www/passwords/passwords
    Require user base
</Directory>
```

After you're done

Go to a shell as root and check everything important to see if it is running.

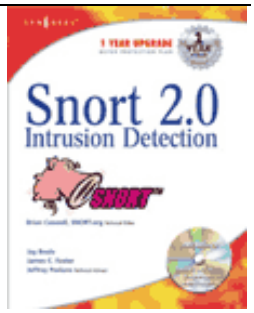
To check you can execute "ps –ef |grep <SERVICE>" where service is snort. httpd, or mysql.

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 BASE 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 BASE 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

Troubleshooting (the Snort install)

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 I get e-mailed with.

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 Fedora 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 BASE again

If you are getting nothing in BASE 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. Scan you box with Nessus or CIS before you start getting worried.

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/ 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, this is free support from the goodness of peoples hearts. They help you out as fast as they can.

Good luck and happy Snorting.

System Hardening – so you don't get r00ted, Coming soon
Barnyard – coming soon as a companion document
OinkMaster - coming soon as a companion document
Openaanval Install - coming soon as a companion document

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.
