Snort_Enterprise_Install

Snort, Apache, SSL, PHP, MySQL, and BASE Install on CentOS 4, RHEL 4 or Fedora Core

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 is really a deviation from what I have done before. It will start from a minimal install of CentOS 4 or RHEL 4 and will build a Snort sensor/manager. This system will start at the command line and not have X window installed unless you add it during the install. Also you can use Fedora with very little change to this doc.

Acknowledgments:

I would like to thank all my friends and the people on the Ntsug-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)

Websites to visit:
http://www.snort.org
http://secureideas.sourceforge.net/
http://www.mysql.com
http://www.php.net
http://www.centos.org
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 CentOS 4:

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/ .

You will start at a grub screen that has boot:, hit enter. Then you can either choose to check your cd's or skip. If you know they are good then skip it otherwise you might want to check them out.

Welcome:
Click next

Language:
English

Keyboard:
U.S. English

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

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 (for tips on setting up snort with two NIC's see the bottom of this doc).

Firewall:
Choose "enable firewall"
Select remote login (SSH) and Web Server (HHTP, HTTPS)

For the SELinux option, move to warn.

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 – unchecked

Gnome Desktop Environment – unchecked

KDE Desktop Environment - unchecked

XFCE - Accept the default unchecked

Applications:

Editors – choose VIM (or anything else you want to use under this tab)

Engineering and Scientific – Accept the default (unchecked)

Graphical Internet – unchecked

Text based internet – checked by default, leave it this way

Office/Productivity – unchecked.

Sound and Video – unchecked

Authoring and Publishing – unchecked

Graphics – make sure it is unchecked

Games and Entertainment – unchecked

Server Section:
Server configuration tools

- Check and leave at the default

Web Server – ONLY the following should be checked

- Crypto-Utils
- Mod_auth_mysql
- Mod_perl
- Mod_ssl
- Php
- Php_mysql
- Webalizer (if you want to be able to view your web 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
- Mysqlclient10
- 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 – leave this unchecked

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 – unchecked:

Printing support – unchecked

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 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:

You are now in runlevel 3 – command line only

Login as root and setup a user account for yourself

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)

groupadd <groupname>
useradd –g <username> <groupname>

Associate a password with this new username

passwd <username>

You will then be asked to enter and then confirm a password. You can now login as a normal user and, if necessary, if you want root privileges, use su – .

Disable unneeded services:
Disable apmd, cups, isdn, netfs, nfslock, pcmcia (unless you are using a laptop), portmap by typing (as root):
Chkconfig <service> off
You will do this for each service to be terminated.

Update your system

We will be using Yum to keep the system up to date. First we will have to import the GPG key. At the command line type:

rpm --import http://mirror.centos.org/centos/RPM-GPG-KEY-CentOS-4

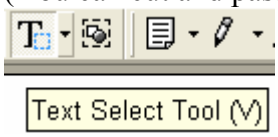
Then type "yum -y update" and it will check what you need and install it.

(Type "chkconfig yum on" and "service yum start" 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 do this from the command line, 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

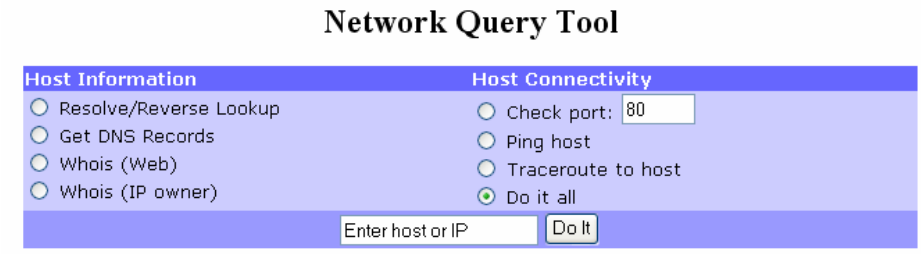
Save the file and type "service sshd restart". SSH will restart, enacting these changes. (You will need to SSH into the box with the user account you created after this, as root will no longer be accepted. Just "su –" to the root account)

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

Install the Network Query Tool, using http://shat.net/php/nqt/nqt.php.txt. Copy the text into a file called query.php and place it in the /var/www/html directory, it will look like the following: this will also tell you if PHP is working correctly



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 command line type:

cd /root
mkdir snortinstall

Remember, you can always check where you are currently by typing "pwd" at the command line. 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!!!

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. This is for windows machines to SSH to Linux/UNIX box's
OR:
http://ftp.ssh.com/pub/ssh/SSHSecureShellClient-3.2.9.exe for a client that can both SSH and start an SCP connection to the box you have SSH'd to from within the session. This is free for non-commercial use and pretty nice.

Download Snort and PCRE

Use wget from the command line or an SSH terminal window. From inside of the /root/snortinstall directory, type:

wget http://www.snort.org/dl/current/snort-2.4.3.tar.gz

When that is downloaded, type:

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

Install PCRE from source

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

Installing and setting up Snort and the Snort rules:

cd back to your snortinstall dir (cd ~/snortinstall)
tar -xvzf snort-2.4.3.tar.gz
cd snort-2.4.3
./configure --with-mysql
make
make install

groupadd snort
useradd -g snort snort –s /sbin/nologin

Then:
mkdir /etc/snort
mkdir /etc/snort/rules
mkdir /var/log/snort

cd etc/
cp * /etc/snort

From your snortinstall dir (cd /root/snortinstall) :
wget http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.4.tar.gz

Then tar –xvzf snortrules-pr-2.4.tar.gz
cd to rules and do the following command
cp –R * /etc/snort/rules

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"

After the line that says "preprocessor stream4_reassemble" add a line that looks like

"preprocessor stream4_reassemble: both,ports 21 23 25 53 80 110 111 139 143 445 513 1433" (without the quotes)

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=<the password you gave it> dbname=snort host=localhost

Get snort start with the system

```
Change directory to /etc/init.d and type:
wget http://internetsecurityguru.com/snortinit/snort
chmod 755 snort
chkconfig snort on.
```

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-2.4.3/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 (cd /root/snortinstall)

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

Download ADODB
wget http://easynews.dl.sourceforge.net/sourceforge/adodb/adodb462.tgz

Download BASE
wget http://easynews.dl.sourceforge.net/sourceforge/secureideas/base-1.2.tar.gz

Hand configure your firewall:
cd /etc/sysconfig/
edit the iptables file
add the line "-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
And delete the lines:
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

Then change the line :
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
To :
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j REJECT

Then you will only be able to get to the site with HTTPS:// the reason you want to do this is so you do not trigger more alerts from you reading alerts, and if something is able to be encrypted then I usually do.

Then execute the command "service iptables restart" and you will see something like tee following:

```
[root@snort conf]# service iptables restart
Flushing firewall rules:                   [  OK  ]
Setting chains to policy ACCEPT: filter    [  OK  ]
Unloading iptables modules:                [  OK  ]
Applying iptables firewall rules:          [  OK  ]
```

Then it will look like this when you do an "iptables –L"

```
[root@snort ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
REJECT     icmp --  anywhere             anywhere            icmp any reject-with icmp-port-unreachable
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            state NEW tcp dpt:https
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited
```

Installing ADODB:

Go back to your download directory (~/snortinstall)
cp adodb462.tgz /var/www/
cd /var/www/
tar -xvzf adodb462.tgz
rm –rf adodb462.tgz

Installing and configuring BASE:

Go back to your download directory (~/snortinstall)
cp base-1.2.tar.gz /var/www/html
cd /var/www/html
tar –xvzf base-1.2.tar.gz
rm –f base-1.2.tar.gz
mv base-1.2 base (this renames the base-1.2 directory to just "base")

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/adodb/ ";
$DBtype = "mysql";

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

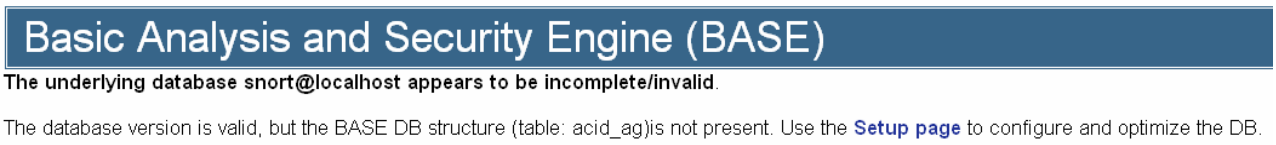
/* Archive DB connection parameters */
$archive_exists = 0; # Set this to 1 if you have an archive DB

Now, go to a browser and access your sensor.

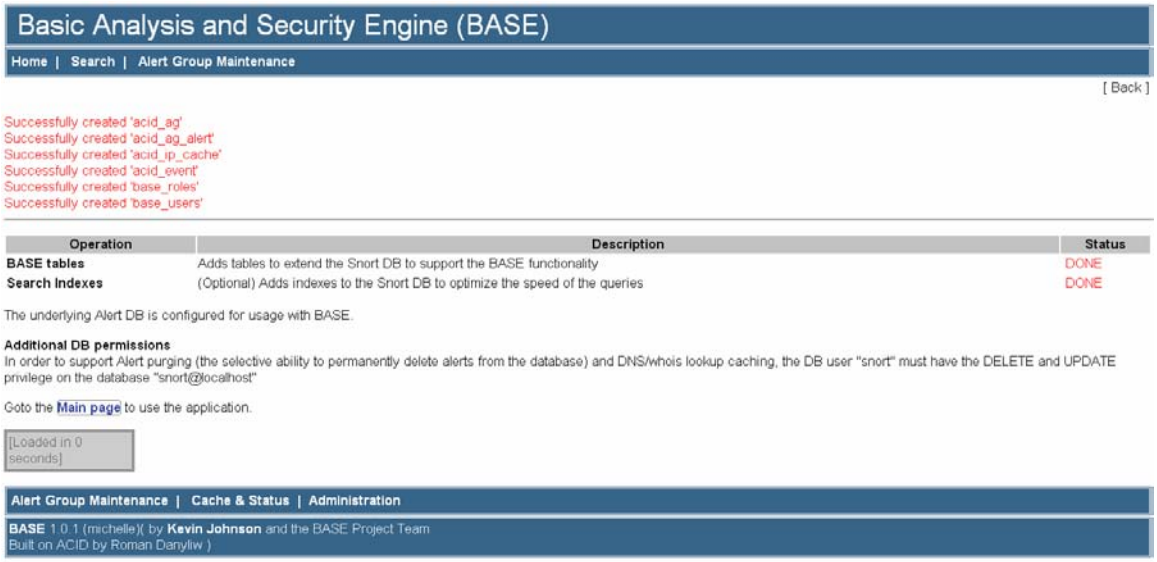
NOW: "chkconfig snort on" to make snort starts with the system
then type service snort start. It should give you an OK

https://<ip.address>/base

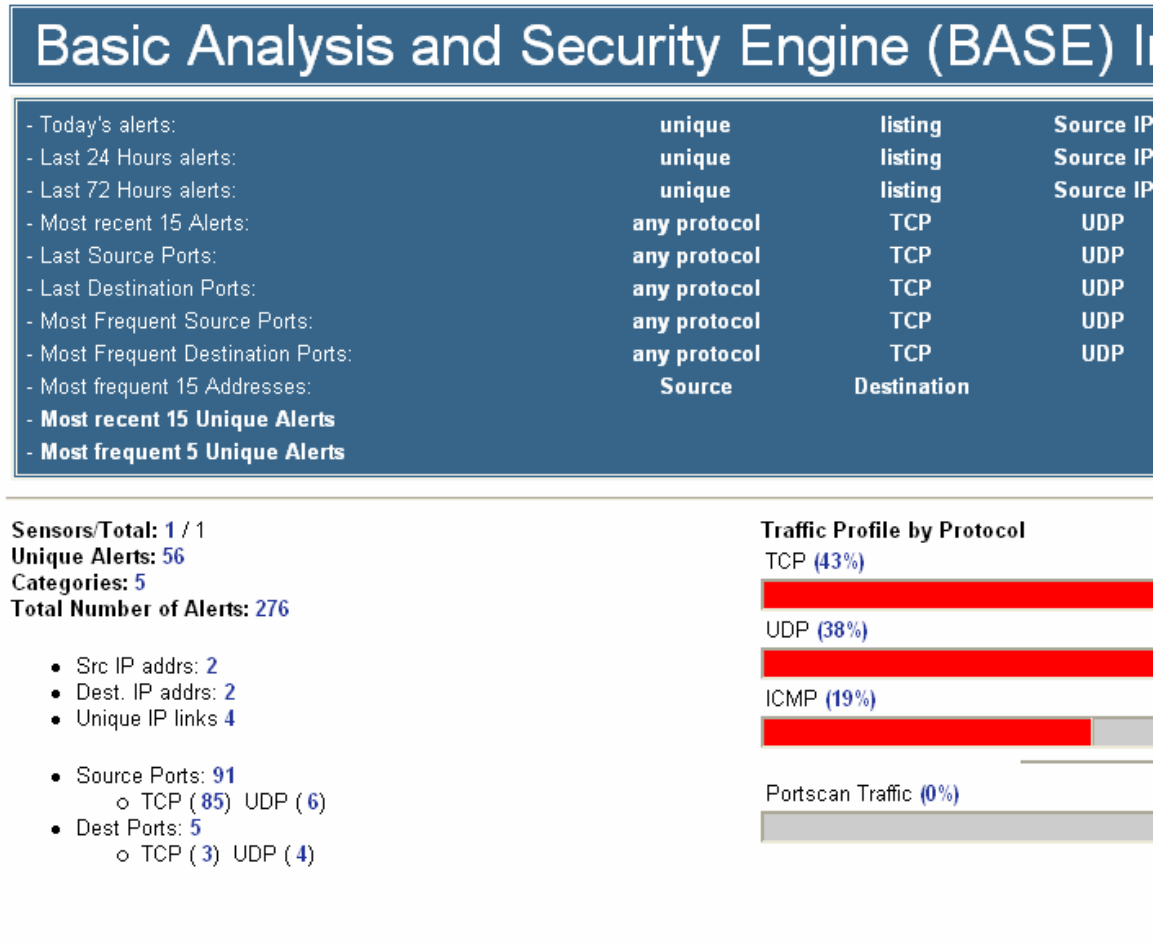
This will bring up the initial BASE startup banner.



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 APACHE and 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 you must add to password protect the BASE console, add it to the httpd.conf file in /etc/httpd/conf/:

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

Since you have removed the port 80 entry in the iptables script you will have to go to the console on port 443, using HTTPS:/<ip_address>/base

Save the file and restart Apache by typing “service httpd restart” to make the password changes effective.

After you’re done

Login 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.

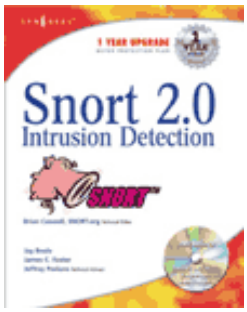
Or use “ps –ef |grep httpd && ps –ef |grep mysql && ps –ef |grep Snort”

Now it’s time to test Snort. I suggest using something free like GFI Languard – a real good program that is cheap (http://www.gfi.com/languard/) or Nessus – a real good program that is free (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.

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.

Two NIC's in the Pig

You may want to have one interface for management and one for sniffing, this is a good thing to do. Here is an example config

cd /etc/sysconfig/network-scripts/

Here you have a file for each of your interfaces (ifcfg-ethX)

For your sniffing interface make the file say the following:

DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet

For your management make it say this: (with your info of course)

DEVICE=ethX
BOOTPROTO=none
HWADDR=00:08:C7:56:E8:87
ONBOOT=yes
TYPE=Ethernet
HOSTNAME=snort.whatever.com
IPADDR=10.10.10.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
GATEWAY=10.10.10.1
IPV6INIT=no

OinkMaster

Please see the OinkMaster install doc on my website

Coming soon is a barnyard doc and a doc on how to deploy multiple sensors with one base station and have them all communicate securely.