Snort_Enterprise_Install

Snort, Apache, SSL, PHP, MySQL, Barnyard and BASE Install on CentOS 5, RHEL 5 or Fedora Core – with NTOP

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 5 or RHEL 5 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 5:

This is a minimal install of CentOS 5.X (or you can use RHEL 5.X with no changes or Fedora Core with few changes) this starts with a minimal install, and then uses yum to add the packages needed. It is suitable for a sensor or a manager. Soon I will have a doc to make a manager with this install and attach remote sensors to it making it the station that accepts all the logs. It also installs NTOP because I find it useful on my sensors to have that to watch who is doing what and going where.

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 /

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).

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)

Packages:
Take the default, it will start to load the system and then do a reboot.

After the reboot you will answer the following questions.

Firewall:
Choose "enable firewall"
Select remote login (SSH) and Secure WWW (HTTPS)
Tell it yes to overwrite the existing firewall config

SELinux:
Set this to Permissive (if you are familiar with SELinux you can keep this on, when you have problems make sure to check /var/log/messages and it will give you an sealert code to run that will help you fix the problem so SELinux will let your app work again)

Date and Time:
Make sure this is correct, setup NTP servers if you have them or you can use the default NTP servers that are in the config

Create a user:
You can setup a user for yourself here

Sound Card:
Self explanatory

Additional CDs:
Hit finish

After the reboot:

Login as root

User Account:
Add more user accounts; make sure to give them 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  <groupname> <username>
```

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 the following services: 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.

Set the system to boot into init 3, this is normally the best thing to do for servers. Edit /etc/inittab and change the line that says **id:5:initdefault:** to say **id:3:initdefault:**

Install needed packages

For NTOP we will be installing from the RPMForge repository, they also have a lot of other software. Download the RPM for your distribution from here http://dag.wieers.com/rpm/FAQ.php#B and use rpm –Uvh to install the RPM for RHEL 5. The RPM that is there at the time I am writing this is http://apt.sw.be/packages/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.i386.rpm. Use wget to download it and use rpm –Uvh to upgrade the existing yum config

We need to remove some unneeded packages, use the following command:

```
yum groupremove "GNOME Desktop Environment" "X Window System" "Graphical Internet" "Games and Entertainment" "Office/Productivity"
```

Then use this line to install all the needed software:

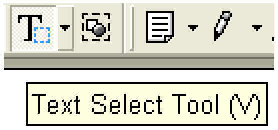
```
yum –y  install mysql mysql-bench mysql-server mysql-devel mysqlclient10 php-mysql httpd gcc pcre-devel php-gd gd mod_ssl glib2-devel gcc-c++ libpcap-devel php php-pear yum-utils
```

Update your system

Type “yum -y update” and it will check what needs updated and install it.

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
```

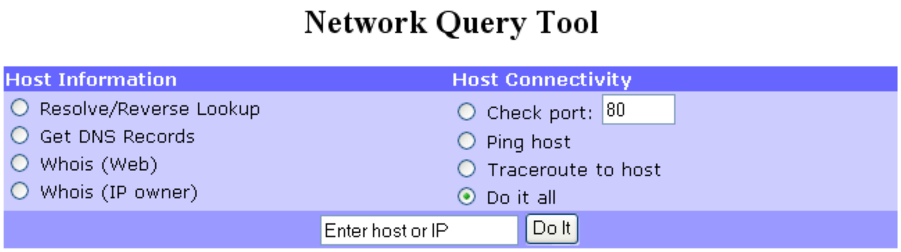
Save the file and type “service sshd restart”. SSH will restart, enacting these changes. (You will need to SSH into the box with the user account you created after this, as root will no longer be accepted. Just “su –“ to the root account)

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

From /var/www/html type “wget http://www.internetsecurityguru.com/index.php.txt”. Move the file to one called index.php, it will look like the following: This will also tell you if PHP is working correctly (originally from http://www.shat.net/php/nqt/) to check if it is working go to https://ip_address (remember port 80 and http are turned off in the firewall)



Network Query Tool

Host Information	Host Connectivity
○ Resolve/Reverse Lookup	○ Check port: 80
○ Get DNS Records	○ Ping host
○ Whois (Web)	○ Traceroute to host
○ Whois (IP owner)	● Do it all

Enter host or IP [Do It]

Download all the needed files:

Remember, you can always check where you are currently by typing “pwd” at the command line. Note: If you aren’t 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 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 boxes or use 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.

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. Create a directory under /root called snortinstall. From the command line type:

```
cd /root
mkdir snortinstall
```

Use your wget from the command line or an SSH terminal window. From inside of /root/snortinstall so all your install files are in one place unless otherwise directed to.

Installing and setting up Snort and the Snort rules:

```
wget http://snort.org/dl/current/snort-2.6.1.5.tar.gz

tar -xvzf snort-2.6.1.5.tar.gz
cd snort-2.6.1.5
./configure --with-mysql --enable-dynamicplugin
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 use pwd to check where you are):

```
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 the rules dir and do the following command
cp * /etc/snort/rules

Modify your snort.conf file

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

var HOME_NET 10.0.0.0/24 (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 a unified file for barnyard

Uncomment (remove the #) from the following lines in the output section of /etc/snort/snort.conf

```
# output alert_unified: filename snort.alert, limit 128
# output log_unified: filename snort.log, limit 128
```

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('pick_a_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
```

Execute the following commands to create the tables

```
mysql -u root -p  <  ~/snortinstall/snort-2.6.1.5/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;
```

Barnyard install

```
cd /root/snortinstall
wget http://snort.org/dl/barnyard/barnyard-0.2.0.tar.gz
```

```
tar –xvzf  barnyard-0.2.0.tar.gz
cd barnyard-0.2.0
./configure --enable-mysql
make
make install
cd etc/
cp barnyard.conf /etc/snort
```

edit /etc/snort/barnyard.conf and make the following changes

uncomment the line that says: # enable daemon mode
change the following to reflect your setup
config hostname: snorthost (sensor1 or snort or whatever you want to use)
config interface: fxp0 (eth0 or eth1 for most setups)

Go to the section labeled # acid_db and uncomment and alter these lines to they fit your parameters. Our database name is snort and our user is snort. You will also have to add password (the password for snort you did in mysql) to the line so they look something like this

```
# output alert_acid_db: mysql, sensor_id 1, database snort, server localhost, user root
# output log_acid_db: mysql, database snort, server localhost, user root, detail full
```

```
output alert_acid_db: mysql, sensor_id 1, database snort, server localhost, user root, password snort
output log_acid_db: mysql, database snort, server localhost, user root, password snort, detail full
```

You have to create a waldo file for barnyard. Do the following “snort –c /etc/snort/snort.conf” and let it get to the part that says Not Using PCAP_FRAMES , let it run for a few seconds and hit ctrl-c to stop it. Look in /var/log/snort and you will see files like this:

```
-rw-------  1 root root   16 Jun 21 07:06 snort.alert.1182427612
-rw-------  1 root root   24 Jun 21 07:06 snort.log.1182427612
```

Type the following: touch /var/log/snort/barnyard.waldo
Then edit the barnyard.waldo file you just created and place the following in it:
/var/log/snort snort.log 1182427612 0 (we used 1182427612 because that was the number appended to the snort.log file in the /var/log/snort directory. Use whatever yours is in the file)

Change to /etc/init.d and type:

```
wget http://www.internetsecurityguru.com/barnyard
chmod 755 barnyard
chkconfig barnyard on
service barnyard start
```

BASE Install

Go to your snort download directory (cd /root/snortinstall)

Then for proper graphing enter:

```
pear install Image_Graph-alpha Image_Canvas-alpha Image_Color
Numbers_Roman
```

Download ADODB

```
wget http://easynews.dl.sourceforge.net/sourceforge/adodb/adodb480.tgz
```

Download BASE

```
wget http://easynews.dl.sourceforge.net/sourceforge/secureideas/base-1.3.5.tar.gz
```

Installing ADODB:

```
cd /var/www/
tar -xvzf /root/snortinstall/adodb480.tgz
```

Installing and configuring BASE:

```
cd /var/www/html
tar –xvzf /root/snortinstall/base-1.3.5.tar.gz
mv base-1.3.5/ base/ (this renames the base-1.3.5 directory to just “base”)
```

Copy the base_conf.php.dist to 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
```

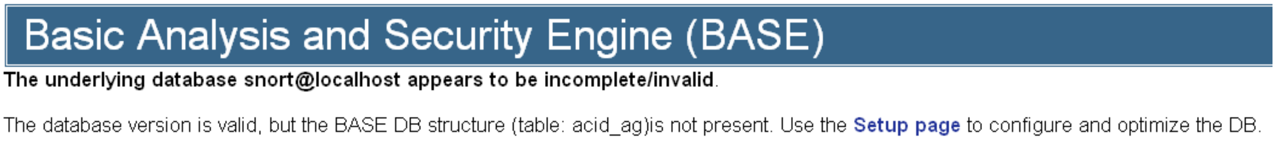
Now, go to a browser and access your sensor.
https://ip_address/base and answer the questions.

NOW: “chkconfig snort on” to make snort starts with the system
Then type “service snort start”. It should give you an OK ps –ef|grep snort.conf will tell

you if it is running or not

https://<ip.address>/base

This will bring up the initial BASE startup banner.

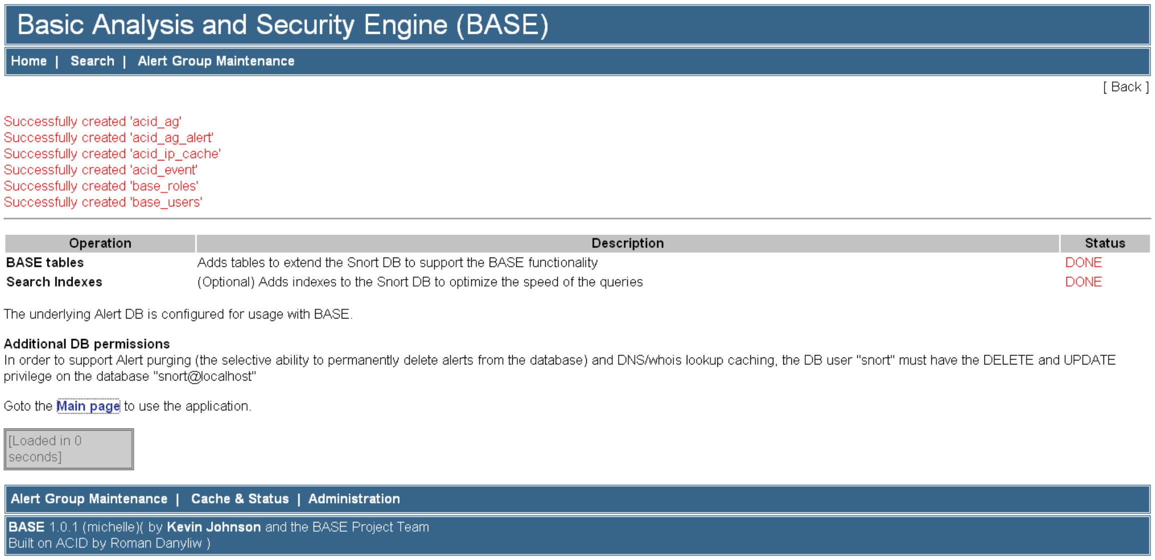


Basic Analysis and Security Engine (BASE)

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

The database version is valid, but the BASE DB structure (table: acid_ag)is not present. Use the **Setup page** to configure and optimize the DB.

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



Basic Analysis and Security Engine (BASE)

Successfully created 'acid_ag'
Successfully created 'acid_ag_alert'
Successfully created 'acid_ip_cache'
Successfully created 'acid_event'
Successfully created 'base_roles'
Successfully created 'base_users'

Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality	DONE
Search Indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

The underlying Alert DB is configured for usage with BASE.

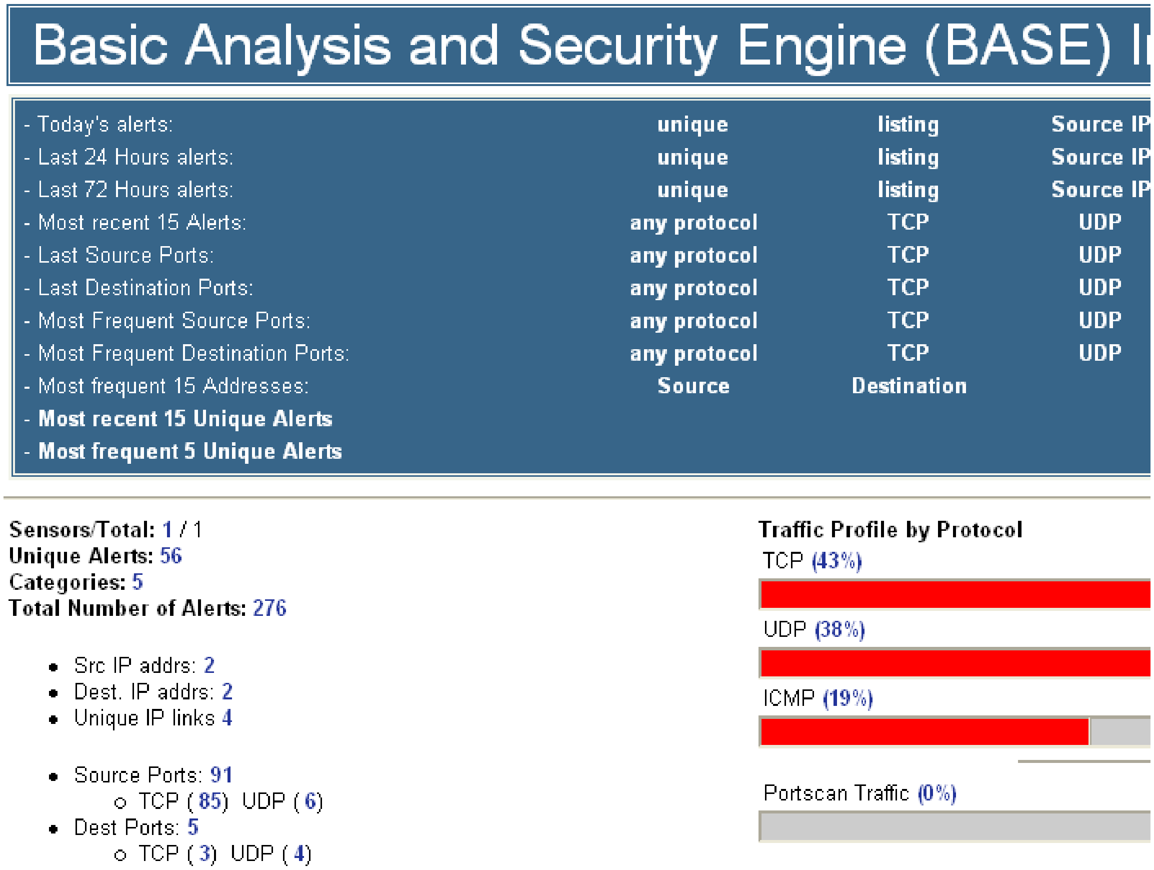
Additional DB permissions
In order to support Alert purging (the selective ability to permanently delete alerts from the database) and DNS/whois lookup caching, the DB user "snort" must have the DELETE and UPDATE privilege on the database "snort@localhost"

Goto the Main page to use the application.

[Loaded in 0 seconds]

BASE 1.0.1 (michelle)(by **Kevin Johnson** and the BASE Project Team
Built on ACID by Roman Danyliw)

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



Basic Analysis and Security Engine (BASE) I

- Today's alerts:	unique	listing	Source IP
- Last 24 Hours alerts:	unique	listing	Source IP
- Last 72 Hours alerts:	unique	listing	Source IP
- Most recent 15 Alerts:	any protocol	TCP	UDP
- Last Source Ports:	any protocol	TCP	UDP
- Last Destination Ports:	any protocol	TCP	UDP
- Most Frequent Source Ports:	any protocol	TCP	UDP
- Most Frequent Destination Ports:	any protocol	TCP	UDP
- Most frequent 15 Addresses:	Source	Destination	
- **Most recent 15 Unique Alerts**			
- **Most frequent 5 Unique Alerts**			

Sensors/Total: 1 / 1
Unique Alerts: 56
Categories: 5
Total Number of Alerts: 276

- Src IP addrs: 2
- Dest. IP addrs: 2
- Unique IP links 4

- Source Ports: 91
  - TCP (85) UDP (6)
- Dest Ports: 5
  - TCP (3) UDP (4)

Traffic Profile by Protocol

TCP (43%)

UDP (38%)

ICMP (19%)

Portscan Traffic (0%)

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 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.

Problem: for right now there is a problem with the pcre in web-misc.rules on Line 452 and the pcre install on CentOS 5. vi the file and enter :452 to go to that line and comment it out.

Set the system up to send root's e-mail to you, edit the aliases file.

```
vi /etc/aliases
```

On the last line in the file uncomment it and remove marc and enter your e-mail address.

```
# Person who should get root's mail
root:          me@mydomain.com
```

Save the file and run the command "newaliases" now you will get the logwatch and cron info as well as any system messages and errors. I normally turn the logwatch to high in the logwatch.conf file too for more info on a daily basis

Install NTOP via Yum

To install type "yum install ntop" (you must have installed the rpmforge RPM

Edit the conf file with vi (vi /etc/ntop.conf) and make the following changes:

Comment out the setting to run in daemon mode
Change --daemon to # --daemon

Set to the NIC you use for sniffing. If you only have one NIC this will be eth0
--interface eth1 (or what ever interface you are using)

Then un-comment the option for port 3001 for SSL

Change #--https-server 3001 to --https-server 3001

Add an entry to iptables for 3001 and restart iptables. (You do this in /etc/sysconfig/iptables):

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3001 -j ACCEPT
```

Put it after the line that says:

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
```

And before the line that says:

```
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
```

Restart iptables with “service iptables restart”

Then:

```
/usr/bin/ntop @/etc/ntop.conf -A
```

Set your password and repeat when asked

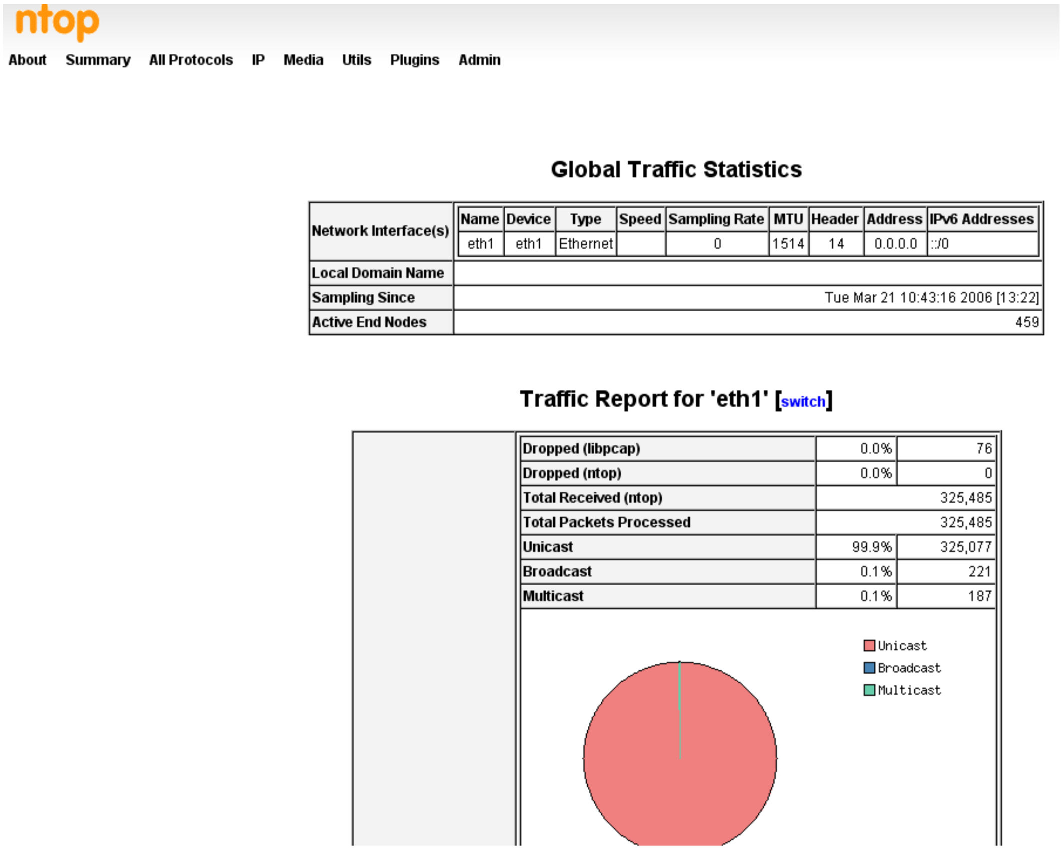
Set back to daemon mode
Change #--daemon to --daemon

Now time to set it to start:

```
chkconfig ntop on
service ntop start
```

Hit it on port 3001 with a web browser. https://<ip_address>:3001

You will see the following; have fun playing around with it. As you will see in the conf file there is more you can play around with. This is a useful tool for me, I hope you find it to be too.



Global Traffic Statistics

Network Interface(s)	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
	eth1	eth1	Ethernet		0	1514	14	0.0.0.0	::/0

Local Domain Name	
Sampling Since	Tue Mar 21 10:43:16 2006 [13:22]
Active End Nodes	459

Traffic Report for 'eth1' [switch]

Dropped (libpcap)	0.0%	76
Dropped (ntop)	0.0%	0
Total Received (ntop)		325,485
Total Packets Processed		325,485
Unicast	99.9%	325,077
Broadcast	0.1%	221
Multicast	0.1%	187

After you're done

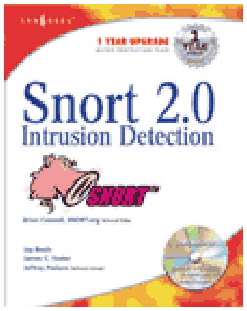
Login as root and check everything important to see if it is running.

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 or on http://www.snort.org

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