Intrusion Detection With BASE And Snort

Intrusion Detection With BASE And Snort

This tutorial shows how to install and configure BASE (Basic Analysis and Security Engine) and the Snort intrusion detection system (IDS) on a Debian Sarge system. BASE provides a web front-end to query and analyze the alerts coming from a Snort IDS system. With BASE you can perform analysis of intrusions that Snort has detected on your network.

Scenario: A linux server running Debian Sarge 3.1 setup according to Falko's - The Perfect Setup - Debian Sarge (3.1).
Let's assume we have one working website (`www.example.com`) and that the document root is: `/var/www/www.example.com/web`
The IP of the server is `192.168.0.5` and it's using `eth0` as network interface name.

Needed programs and files

- Snort
- Snort rules
- PCRE (Perl Compatible Regular Expressions)
- LIBPCAP
- BASE (Basic Analysis and Security Engine)
- ADOdb (ADOdb Database Abstraction Library for PHP (and Python).)

Downloading and untaring

We need a temporary place for all the files that we are going to download, and untar.
To keep things simple we will create a directory in the `/root` named `snorttemp`. (It's obvious that this download directory can be any name and in anyplace)

```
cd /root
mkdir snorttemp
cd snorttemp
```

Now you need to get Snort.
The latest version at the time of writing this is 2.6.0

```
wget http://www.snort.org/dl/current/snort-2.6.0.tar.gz
```

When the download is finished untar the file:

```
tar -xvzf snort-2.6.0.tar.gz
```

And let’s remove the tar file:

```
rm snort-2.6.0.tar.gz
```

We also need the Snort rules!
Go to: http://www.snort.org/pub-bin/downloads.cgi and scroll down till you see the

"Sourcefire VRT Certified Rules - The Official Snort Ruleset (unregistered user release)" rules
(If you are a member of the forum you can also download the - registered user release):

```
wget
http://www.snort.org/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.4.tar.gz
```

Move the `snortrules-pr-2.4.tar.gz` into the `snort-2.6.0` map:

```
mv snortrules-pr-2.4.tar.gz /root/snorttemp/snort-2.6.0
```

and cd into `snort-2.6.0`:

```
cd snort-2.6.0
```

Untar the `snortrules-pr-2.4.tar.gz` file:

```
tar -xvzf snortrules-pr-2.4.tar.gz
```

Remove the tar file:

```
rm snortrules-pr-2.4.tar.gz
```

We are done downloading the files needed to get Snort to work.

To make snort work with BASE, we need more!

PCRE - Perl Compatible Regular Expressions.

Go to: http://www.pcre.org/ and select a download link for the `pcre-6.3tar.gz` file to download PCRE (at time of writing this it is `pcre-6.3.tar.gz`)
cd back to the snorttemp map:

```
cd /root/snorttemp
```

and download the `pcre-6.3.tar.gz` file:

```
wget http://surfnet.dl.sourceforge.net/sourceforge/pcre/pcre-6.3.tar.gz
```

Untar the file:

```
tar -xvzf pcre-6.3.tar.gz
```

Remove the tar:

```
rm pcre-6.3.tar.gz
```

Intrusion Detection With BASE And Snort - Page 2

LIBPCAP

Go to: http://www.tcpdump.org/ and select a download link for Libpcap (at time of writing this it is `libpcap-0.9.4.tar.gz`)
cd back to the snorttemp map:

```
cd /root/snorttemp
```

and download the `libpcap-0.9.4.tar.gz` file:

```
wget http://www.tcpdump.org/release/libpcap-0.9.4.tar.gz
```

Untar the file:

```
tar -xvzf libpcap-0.9.4.tar.gz
```

Remove the file:

```
rm libpcap-0.9.4.tar.gz
```

BASE (Basic Analysis and Security Engine)

Go to: http://secureideas.sourceforge.net/ and download the latest release (at time of writing BASE 1.2.5 (sarah))
cd back to the snorttemp map:

```
cd /root/snorttemp
```

and download the `base-1.2.5.tar.gz` file:

```
wget
http://surfnet.dl.sourceforge.net/sourceforge/secureideas/base-1.2.5.tar.gz
```

Untar the file:

```
tar -xvzf base-1.2.5.tar.gz
```

Remove the file:

```
rm base-1.2.5.tar.gz
```

ADOdb: (ADOdb Database Abstraction Library for PHP (and Python).)

Go to: http://adodb.sourceforge.net/ and download the latest release (at time of writing adodb-490-for-php)
cd back to the snorttemp map:

```
cd /root/snorttemp
```

and download the `adodb490.tgz` file:

```
wget http://surfnet.dl.sourceforge.net/sourceforge/adodb/adodb490.tgz
```

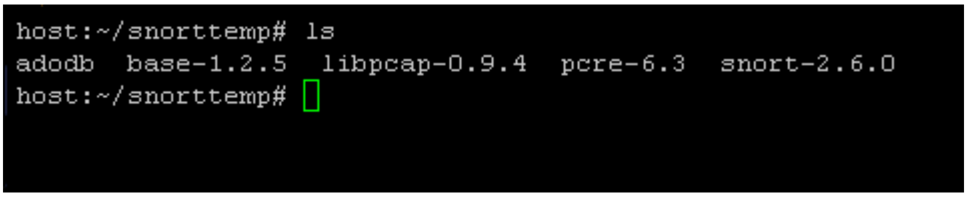
Untar the file:

```
tar -xvzf adodb490.tgz
```

Remove the file:

```
rm adodb490.tgz
```

`ls` should now show the following directorys in `/root/snorttemp`: `adodb`, `base-1.2.5`, `libpcap-0.9.4`, `pcre-6.3` and `snort-2.6.0`



```
host:~/snorttemp# ls
adodb  base-1.2.5  libpcap-0.9.4  pcre-6.3  snort-2.6.0
host:~/snorttemp#
```

Intrusion Detection With BASE And Snort - Page 3

Installing

Lets start with: LIBPCAP.

Make sure that you are in the directory that you downloaded all files.

```
cd /root/snorttemp
```

cd into the libcap map:

```
cd libpcap-0.9.4
```

and make / install LIBPCAP:

```
./configure
make
make install
```

Next is PCRE.
Again, make sure that you are in the directory that you downloaded all files.

```
cd /root/snorttemp
```

cd into the PCRE map:

```
cd pcre-6.3
```

and make / install pce-6.3

```
./configure
make
make install
```

Now it time for Snort:
Make sure that you are in the directory that you downloaded all files.

```
cd /root/snorttemp
```

cd into the snort map:

```
cd snort-2.6.0
```

and make / install Snort with some extra needed options!

```
./configure --enable-dynamicplugin --with-mysql
make
make install
```

Snort needs some maps, so let’s create them:

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

Moving the Snort files from the installation map to the just created maps.
Make sure that you are in the directory that you downloaded all files.

```
cd /root/snorttemp
```

and cd into snort-2.6.0:

```
cd snort-2.6.0
```

and into the rules

```
cd rules
```

now we copy all files from the `/rules` into `/etc/snort/rules`

```
cp * /etc/snort/rules
```

We will do the same for the files in the install `/etc` folder:

```
cd ../etc
cp * /etc/snort
```

Fixing the snort.conf

The `/etc/snort/snort.conf` needs some tuning to get it to work on your system!
So cd into /etc/snort:

```
cd /etc/snort
```

and open snort.conf with nano (or any other 'text' editor)

```
nano snort.conf
```

change `"var HOME_NET any"` to `"var HOME_NET` **`192.168.0.5/32`**`"`
change `"var EXTERNAL_NET any"` to `"var EXTERNAL_NET` **`!$HOME_NET`**`"`
change `"var RULE_PATH ../rules"` to `"var RULE_PATH` **`/etc/snort/rules`**`"`

As we made snort with the `'--with-mysql'` option and as BASE needs it, we also need to tell Snort what database to use.
Scroll down till you see **`"# output database"`**, and **remove** the # in front of the line for the MySQL.
Now also change the "**user**", "**password**" and "**dbname**". ❗ Make a note of this as you will need it later!
Save the file and close 'nano'

Setting up the MySQL Database for Snort.

There are many ways to create the snort database.
The table layout can be found in the file `create_mysql` in the `/root/snorttemp/snort-2.6.0/schemas` directory.
Whichever way you create the database, make sure the **'user'**, **'password'** and **'dbame'** are the same as the one you set in the `/etc/snort/snort.conf` file!

After creating you can test snort and see if you get any errors with:

```
snort -c /etc/snort/snort.conf
```

Exit the test with **Ctrl+C**

If you get no error's Snort is setup correct.

Moving ADOdb and BASE

Moving ADOdb:
cd back to the download dir

```
cd /root/snorttemp/
```

and move adodb it to the root of the www map:

```
mv adodb /var/www
```

Next: BASE (Basic Analysis and Security Engine)
Still in the download dir, we move the base dir into the 1st website map that you create with ISPconfig.

```
mv base-1.2.5 /var/www/www.example.com/web
```

and cd into `/var/www/www.example.com/web`

```
cd /var/www/www.example.com/web
```

To enable BASE to write the setup file we need to chmod the base-1.2.5 folder to 757:

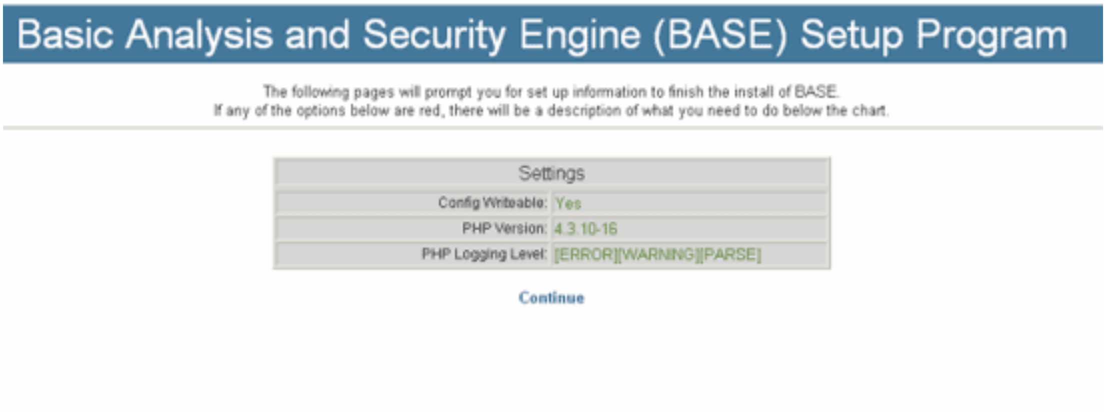
```
chmod 757 base-1.2.5
```

Intrusion Detection With BASE And Snort

- Page 4

BASE web page setup

Open your favorite web browser and go to: `http://www.example.com/base-1.2.5/setup`
If all is setup okay you should see the BASE Setup Program page:



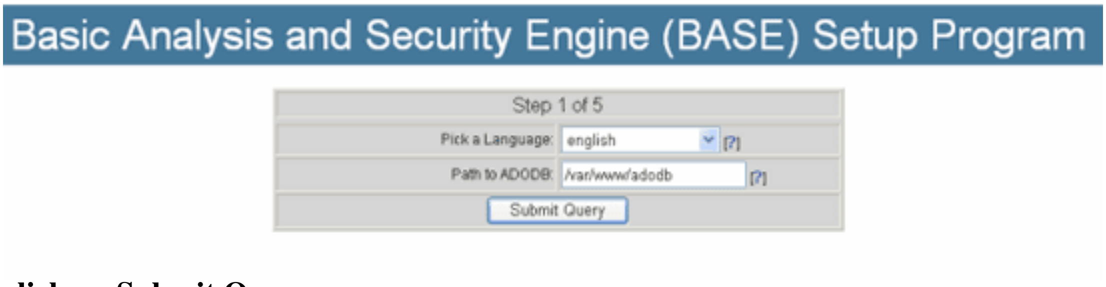
Basic Analysis and Security Engine (BASE) Setup Program

The following pages will prompt you for set up information to finish the install of BASE.
If any of the options below are red, there will be a description of what you need to do below the chart.

Settings	
Config Writeable:	Yes
PHP Version:	4.3.10-16
PHP Logging Level:	[ERROR][WARNING][PARSE]

Click on Continue

step 1 of 5:
Enter the path to ADODB (`/var/www/adodb`):

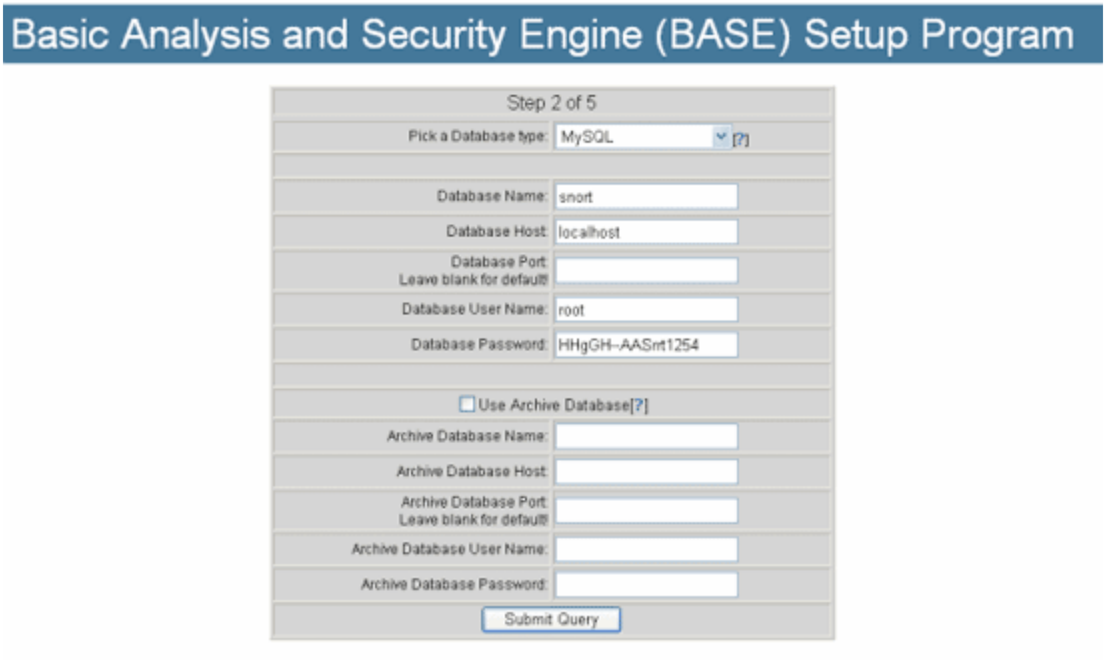


Basic Analysis and Security Engine (BASE) Setup Program

Step 1 of 5	
Pick a Language:	english [?]
Path to ADODB:	/var/www/adodb [?]

click on Submit Query

step 2 of 5:
Enter the needed info on the next screen: (leave the Use Archive Database as is):



Basic Analysis and Security Engine (BASE) Setup Program

Step 2 of 5

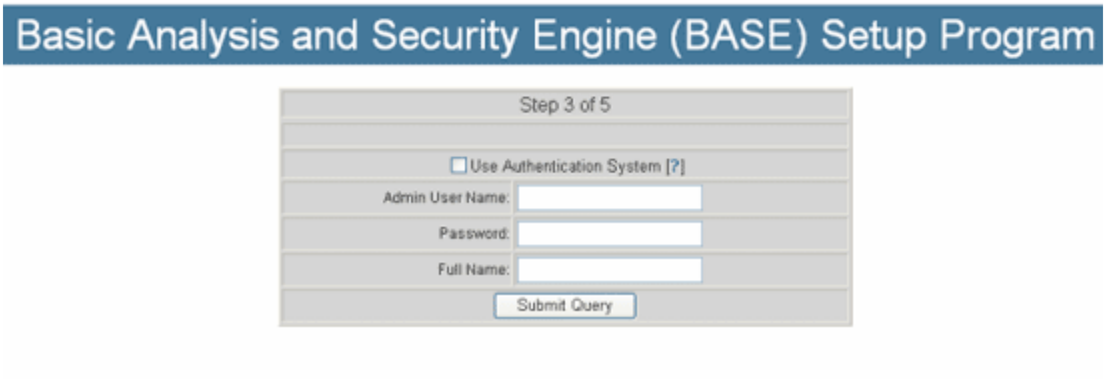
Pick a Database type:	MySQL [?]
Database Name:	snort
Database Host:	localhost
Database Port: Leave blank for default!	
Database User Name:	root
Database Password:	HHgGH--AASnt1254

□ Use Archive Database[?]

Archive Database Name:	
Archive Database Host:	
Archive Database Port: Leave blank for default!	
Archive Database User Name:	
Archive Database Password:	

click on Submit Query

step 3 of 5:
If you want to Use Authentication for the Base page you can do so here:



Basic Analysis and Security Engine (BASE) Setup Program

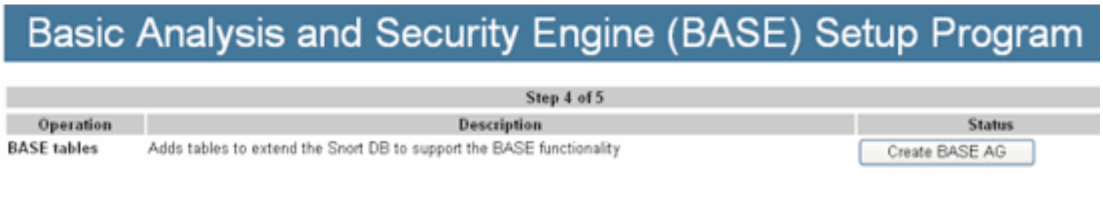
Step 3 of 5

□ Use Authentication System [?]

Admin User Name:	
Password:	
Full Name:	

click on Submit Query

step 4 of 5:
Click on `Create BASE AG` to create the database.

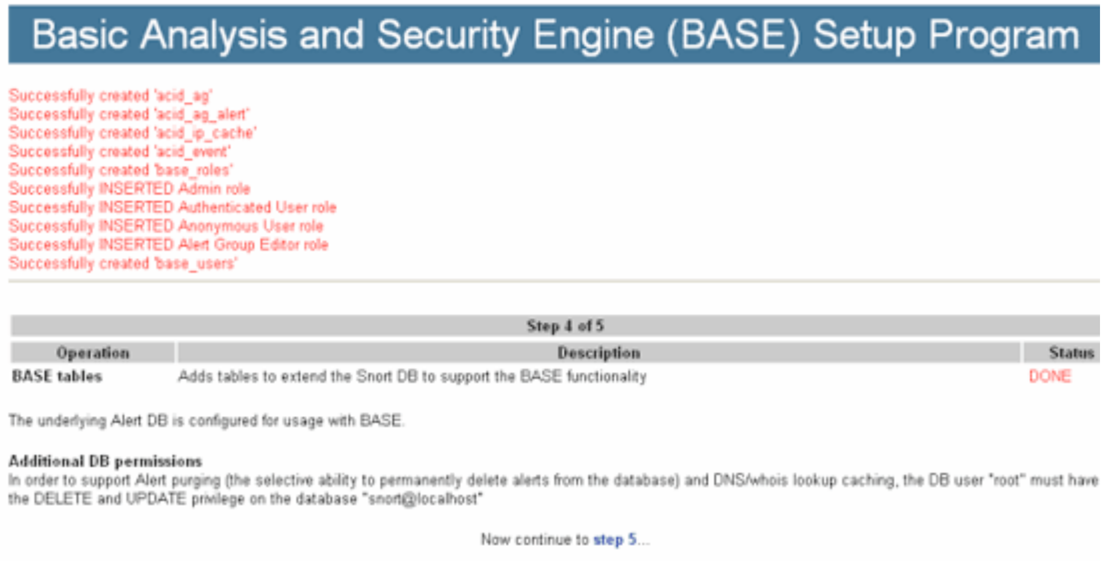


Basic Analysis and Security Engine (BASE) Setup Program

Step 4 of 5

Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality	Create BASE AG

and after `Create BASE AG`



Basic Analysis and Security Engine (BASE) Setup Program

Successfully created 'acid_ag'
Successfully created 'acid_ag_alert'
Successfully created 'acid_ip_cache'
Successfully created 'acid_event'
Successfully created 'base_roles'
Successfully INSERTED Admin role
Successfully INSERTED Authenticated User role
Successfully INSERTED Anonymous User role
Successfully INSERTED Alert Group Editor role
Successfully created 'base_users'

Step 4 of 5

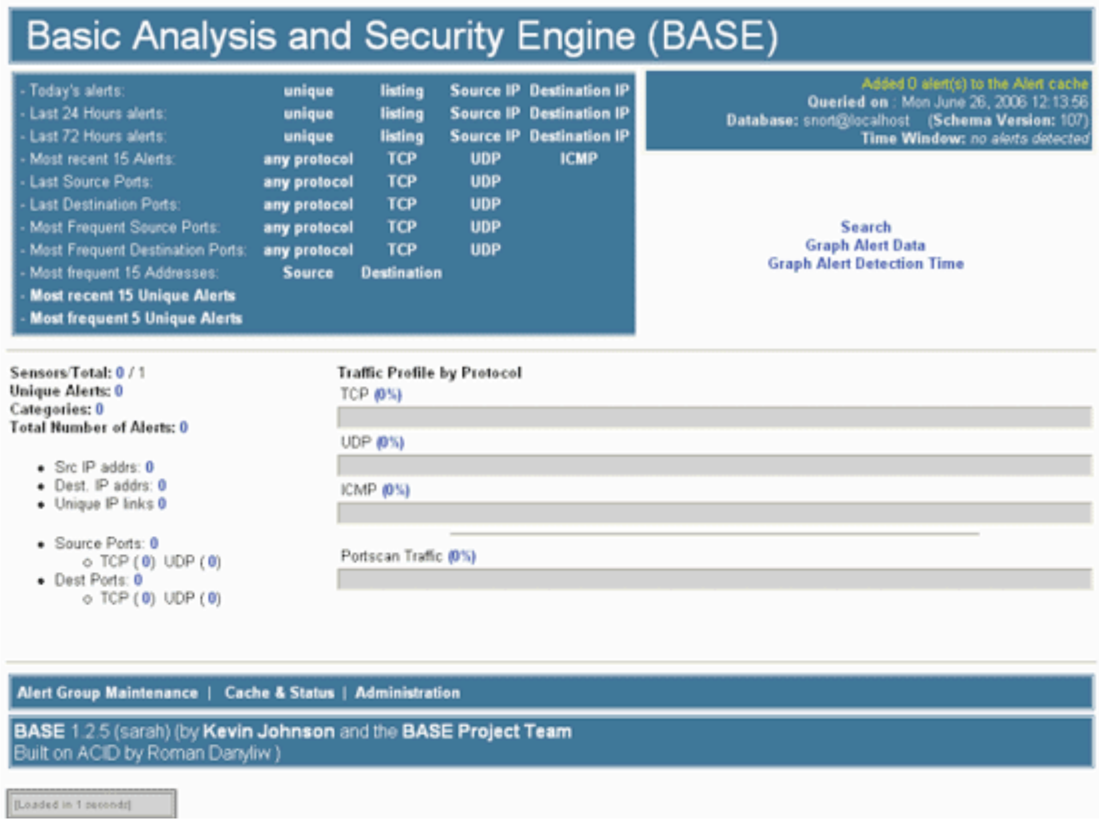
Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality	DONE

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 "root" must have the DELETE and UPDATE privilege on the database "snort@localhost"

Now continue to **step 5**...

Once done, click on `Now continue to step 5...`



Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- 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**				

Added 0 alert(s) to the Alert cache
Queried on : Mon June 26, 2006 12:13:56
Database: snort@localhost (**Schema Version:** 107)
Time Window: *no alerts detected*

Search
Graph Alert Data
Graph Alert Detection Time

Sensors/Total: 0 / 1
Unique Alerts: 0
Categories: 0
Total Number of Alerts: 0

- Src IP addrs: 0
- Dest. IP addrs: 0
- Unique IP links 0

- Source Ports: 0
  - TCP (0) UDP (0)
- Dest Ports: 0
  - TCP (0) UDP (0)

Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (0%)

Portscan Traffic (0%)

Alert Group Maintenance | **Cache & Status** | **Administration**

BASE 1.2.5 (sarah) (by **Kevin Johnson** and the **BASE Project Team**
Built on ACID by Roman Danyliw)

[Loaded in 1 seconds]

To make the Graph's from BASE work you will also need to install `Image_Color`, `Image_Canvas` and `Image_Graph`.
To do this do:

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

That it for BASE!

If you want you can chmod the base-1.2.5 dir back to 775:

```
chmod 775 base-1.2.5
```

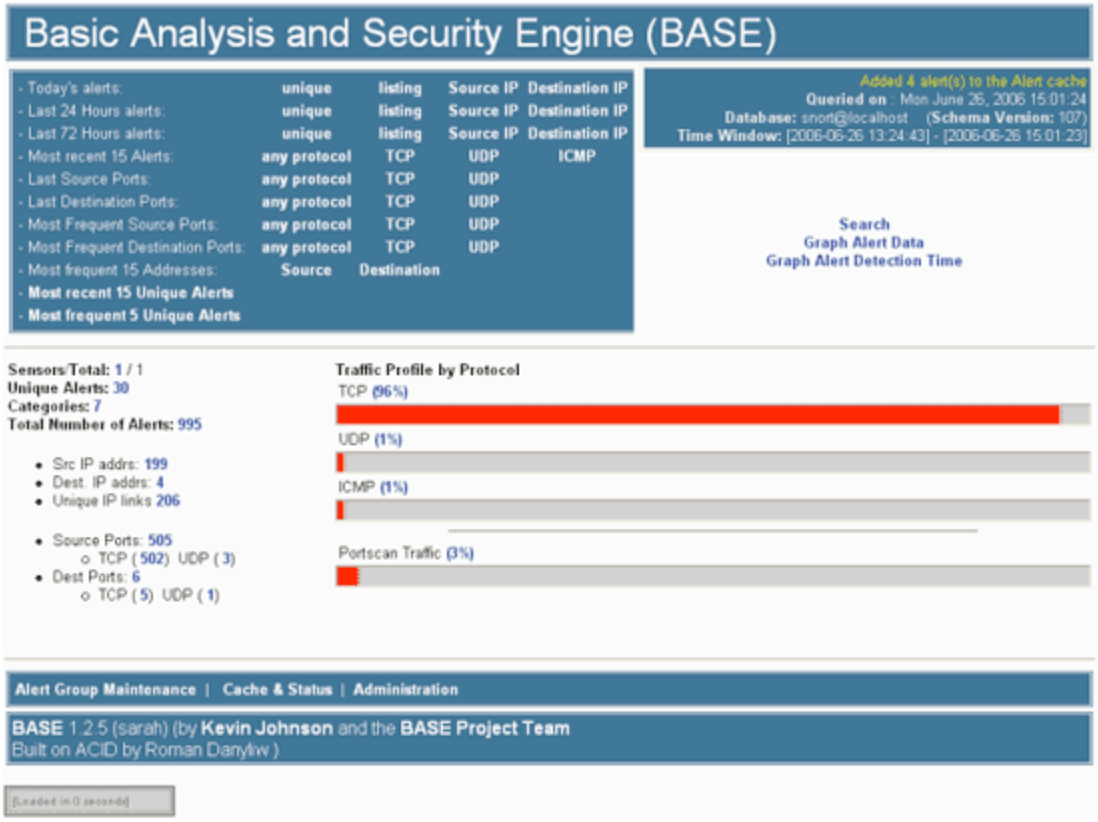
You can also delete the snorttemp directory, and all the files in it.

Starting Snort

To start SNORT and make BASE show you the Snort's logged info, you will need to run:

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

Now wait some time and see all the Snort alerts show up in BASE.



Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- 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**				

Added 4 alert(s) to the Alert cache
Queried on : Mon June 26, 2006 15:01:24
Database: snort@localhost (**Schema Version:** 107)
Time Window: [2006-06-26 13:24:43] - [2006-06-26 15:01:23]

Search
Graph Alert Data
Graph Alert Detection Time

Sensors/Total: 1 / 1
Unique Alerts: 30
Categories: 7
Total Number of Alerts: 995

- Src IP addrs: 199
- Dest. IP addrs: 4
- Unique IP links 206

- Source Ports: 505
  - TCP (502) UDP (3)
- Dest Ports: 6
  - TCP (5) UDP (1)

Traffic Profile by Protocol

TCP (96%)

UDP (1%)

ICMP (1%)

Portscan Traffic (3%)

Alert Group Maintenance | **Cache & Status** | **Administration**

BASE 1.2.5 (sarah) (by **Kevin Johnson** and the **BASE Project Team**
Built on ACID by Roman Danyliw)

[Loaded in 0 seconds]

Links

- BASE: http://secureideas.sourceforge.net
- Snort: http://www.snort.org