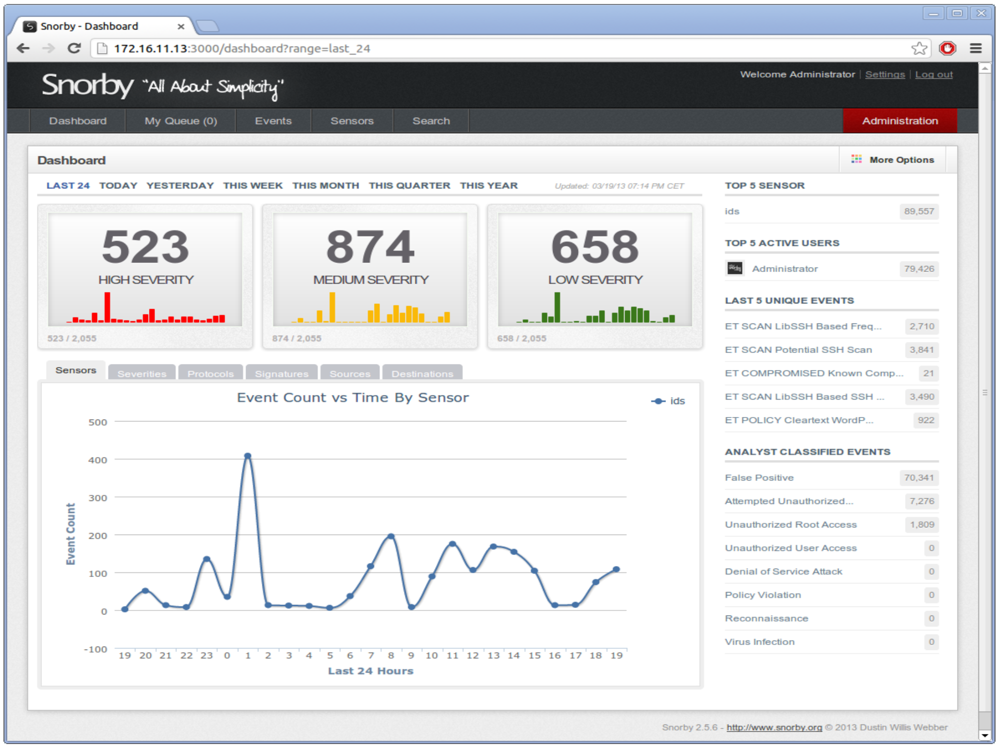
Installation of the SIEM server

This system is used to collect data from any IDS. It uses Snorby as a SIEM to review IDS alerts.



TOP 5 SENSOR

ids	89,557

TOP 5 ACTIVE USERS

Administrator	79,426

LAST 5 UNIQUE EVENTS

ET SCAN LibSSH Based Freq...	2,710
ET SCAN Potential SSH Scan	3,841
ET COMPROMISED Known Comp...	21
ET SCAN LibSSH Based SSH ...	3,490
ET POLICY Cleartext WordP...	922

ANALYST CLASSIFIED EVENTS

False Positive	70,341
Attempted Unauthorized...	7,276
Unauthorized Root Access	1,809
Unauthorized User Access	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0

Installation (Already completed)

The following has already been installed to support the SIEM server:

The key for passenger has been added with the following commands:

apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 561F9B9CAC40B2F7 && apt-get install -y apt-transport-https ca-certificates

sh -c 'echo deb https://oss-binaries.phusionpassenger.com/apt/passenger precise main > /etc/apt/sources.list.d/passenger.list'

The following packages have been installed:
apt-get install mysql-server libyaml-dev git-core default-jre imagemagick libmagickwand-dev wkhtmltopdf build-essential libssl-dev libreadline-gplv2-dev zlib1g-dev linux-headers-amd64 libsqlite3-dev libxslt1-dev libxml2-dev libmysqlclient-dev libmysql++-dev apache2-prefork-dev

libcurl4-openssl-dev ruby ruby-dev apache2 libapache2-mod-passenger postgresql-9.4 postgresql-server-dev-9.4 libpq-dev vim –y

The following additional packages have been installed:
gem install bundler rails
gem install rake --version=0.9.2

Snorby has been downloaded to:
/usr/local/src/
with the following command:
git clone http://github.com/Snorby/snorby.git

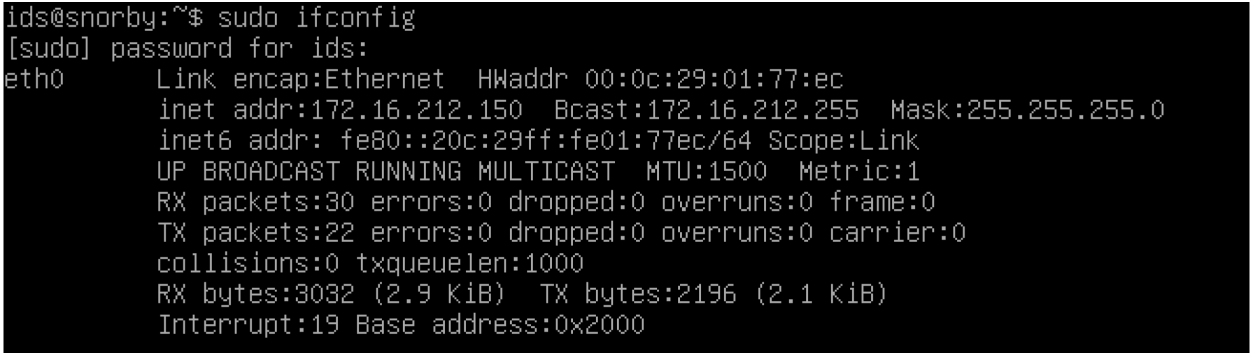
The following command has been run to download all the needed files for Snorby from within the /usr/local/src/snorby directory:
bundle install

Start point:

Start the Virtual Machine
Username: ids
Password: ids

If possible, ssh to the machine to enable copy/paste and for a better interface.
To find out the IP address of the machine, run the following command in the VM:
sudo ifconfig

A screen similar to the following will be displayed:



```
ids@snorby:~$ sudo ifconfig
[sudo] password for ids:
eth0      Link encap:Ethernet  HWaddr 00:0c:29:01:77:ec
          inet addr:172.16.212.150  Bcast:172.16.212.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe01:77ec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3032 (2.9 KiB)  TX bytes:2196 (2.1 KiB)
          Interrupt:19 Base address:0x2000
```

Once logged in, copy the Snorby source to its working directory:
sudo cp -R /usr/local/src/snorby /var/www/snorby

Change permissions so we can work with it correctly:
sudo chown -R ids:ids /var/www/snorby

Change into that directory:

```
cd /var/www/snorby
```

Copy the database.yml.example and snorby_config.yml files to working files:

```
cp config/database.yml.example config/database.yml
cp config/snorby_config.yml.example config/snorby_config.yml
```

Modify the /var/www/snorby/config/database.yml file to look like the following:

```
snorby: &snorby
  adapter: mysql
  username: snorby
  password: "p@55word"
  host: localhost
```

Create the MySQL database to store alerts. Barnyard on the IDS systems will be sending to this database:

```
mysql -uroot –p
```

Use the mysql password: ‘ids’

Enter the following commands:

```
create database snorby;
create user 'snorby'@'localhost' identified by 'p@55word';
grant all privileges on snorby.* to 'snorby'@'%' identified by 'p@55word' require ssl;
flush privileges;
exit;
```

Create the certificates for secure transfer over MySQL:

```
mkdir openssl openssl/private openssl/newcerts
cp /etc/ssl/openssl.cnf openssl
```

In openssl/openssl.cnf, replace all instances of 'demoCA' with 'openssl'

```
sed -i 's/demoCA/openssl/g' openssl/openssl.cnf
```

Create necessary files: $database, $serial and $new_certs_dir

```
touch openssl/index.txt
echo "01" > openssl/serial
```

Generation of Certificate Authority(CA)

```
openssl req -new -x509 -keyout openssl/private/cakey.pem -out openssl/ca-cert.pem -days
3600 -config openssl/openssl.cnf -passout pass:supereasypassword -subj
"/C=US/ST=CA/L=Portland/O=BSides/OU=BSides/CN=BSides
CA/emailAddress=BSides@BSides.com"
```

Create server request and key

```
openssl req -new -keyout openssl/server-key.pem -out openssl/server-req.pem -days 3600 -
config openssl/openssl.cnf -passout pass:supereasypassword -subj
"/C=US/ST=CA/L=Portland/O=BSides/OU=BSides/CN=BSides
Server/emailAddress=BSides@BSides.com"
```

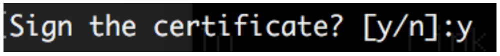
Remove the passphrase from the key

```
openssl rsa -in openssl/server-key.pem -out openssl/server-key.pem -passout
pass:supereasypassword
```

Sign server cert

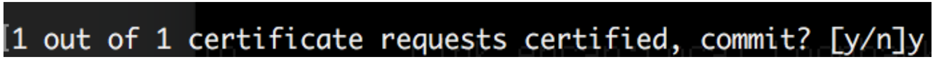
```
openssl ca -cert openssl/ca-cert.pem -policy policy_anything -out openssl/server-cert.pem -
config openssl/openssl.cnf -infiles openssl/server-req.pem
```

Enter 'y' when asked to sign the certificate:



```
Sign the certificate? [y/n]:y
```

Enter 'y' when asked to commit the certificate:



```
1 out of 1 certificate requests certified, commit? [y/n]y
```

Create client request and key:

```
openssl req -new -keyout openssl/client-key.pem -out \
   openssl/client-req.pem -days 3600 -config openssl/openssl.cnf \
   -passout pass:supereasypassword -subj
"/C=US/ST=CA/L=Portland/O=BSides/OU=BSides/CN=BSides
Client/emailAddress=BSides@BSides.com"
```

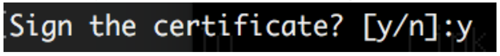
Remove the passphrase from the key:

```
openssl rsa -in openssl/client-key.pem -out openssl/client-key.pem -passout
pass:supereasypassword
```

Sign client certificate:

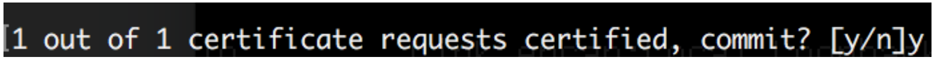
```
openssl ca -cert openssl/ca-cert.pem -policy policy_anything -out openssl/client-cert.pem -
config openssl/openssl.cnf -infiles openssl/client-req.pem
```

Enter 'y' when asked to sign the certificate:



```
Sign the certificate? [y/n]:y
```

Enter 'y' when asked to commit the certificate:



```
1 out of 1 certificate requests certified, commit? [y/n]y
```

Run the following to save the details you'll need to add to the MySQL configuration on each system:

```
cat <<EOF > openssl/my.cnf
[client]
ssl-ca=/usr/local/certificates/openssl/ca-cert.pem
ssl-cert=/usr/local/certificates/openssl/client-cert.pem
ssl-key=/usr/local/certificates/openssl/client-key.pem
[mysqld]
ssl-ca=/usr/local/certificates/openssl/ca-cert.pem
ssl-cert=/usr/local/certificates/openssl/server-cert.pem
ssl-key=/usr/local/certificates/openssl/server-key.pem
EOF
```

Move everything to a permanent directory:

```
sudo mkdir -p /usr/local/certificates && sudo mv openssl /usr/local/certificates/
```

Add to /etc/mysql/my.cnf, under the [mysqld] section:

```
ssl-ca=/usr/local/certificates/openssl/cacert.pem
ssl-cert=/usr/local/certificates/openssl/client-cert.pem
ssl-key=/usr/local/certificates/openssl/client-key.pem
```

Set the bind address to the IP address of the system you are currently on:

```
bind-address = IP ADDRESS
```

Restart mysql:

```
sudo service mysql restart
```

Modify the apache sites configuration file:

```
sudo vim /etc/apache2/sites-enabled/000-default.conf
```

Remove the current entries and add the following:

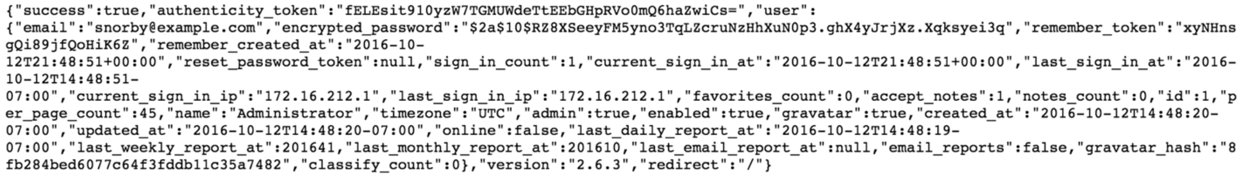
```
<VirtualHost *:80>
  ServerName snorby
  # !!! Be sure to point DocumentRoot to 'public'!
  DocumentRoot /var/www/snorby/public
  <Directory /var/www/snorby/public>
    # This relaxes Apache security settings.
    AllowOverride all
    # MultiViews must be turned off.
    Options -MultiViews
  </Directory>
</VirtualHost>
```

Restart Apache:
sudo service apache2 restart

From inside the /var/www/snorby directory, run bundle install and configure the database for Snorby:
bundle install
bundle exec rake snorby:setup

Open a browser and go to the IP address of the VM to log into Snorby:
snorby@example.com
snorby

Note: This has been fixed prior to setting this up, but for future reference:
If after logging in, you get a message like this:



```
{"success":true,"authenticity_token":"fELEsit910yzW7TGMUWdeTtEEbGHpRVo0mQ6haZwiCs=","user":
{"email":"snorby@example.com","encrypted_password":"$2a$10$RZ8XSeeyFM5yno3TqLZcruNzHhXuN0p3.ghX4yJrjXz.Xqksyei3q","remember_token":"xyNHns
gQi89jfQoHiK6Z","remember_created_at":"2016-10-
12T21:48:51+00:00","reset_password_token":null,"sign_in_count":1,"current_sign_in_at":"2016-10-12T21:48:51+00:00","last_sign_in_at":"2016-
10-12T14:48:51-
07:00","current_sign_in_ip":"172.16.212.1","last_sign_in_ip":"172.16.212.1","favorites_count":0,"accept_notes":1,"notes_count":0,"id":1,"p
er_page_count":45,"name":"Administrator","timezone":"UTC","admin":true,"enabled":true,"gravatar":true,"created_at":"2016-10-12T14:48:20-
07:00","updated_at":"2016-10-12T14:48:20-07:00","online":false,"last_daily_report_at":"2016-10-12T14:48:19-
07:00","last_weekly_report_at":201641,"last_monthly_report_at":201610,"last_email_report_at":null,"email_reports":false,"gravatar_hash":"8
fb284bed6077c64f3fddb11c35a7482","classify_count":0},"version":"2.6.3","redirect":"/"}
```

Edit /var/www/snorby/public/assets/snorby.js
Add the following to the next new line:
form#new_user