Installing Snorby on Debian 6.0 (Squeeze)

Miguel Angel Cabrerizo, `doncicuto[at]gmail.com`

v1, 1 November 2011

---

1. Introduction

According to snorby.org, Snorby is a ruby on rails web application for network security monitoring that interfaces with current popular intrusion detection systems (Snort, Suricata and Sagan). The project goal is to create a free, open source and highly competitive application for network monitoring for both private and enterprise use.

Today I'm going to show you how to install Snorby on Debian 6. This is the first time I use Snorby so I'll post my first impressions.

1.1 Copyright

This document is Copyright 2011 by Miguel Angel Cabrerizo. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.1 or any later version published by the Free Software Foundation with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

1.2 Disclaimer

Use the information in this document at your own risk. I disavow any potential liability for the contents of this document. Use of the concepts, examples, and/or other content of this document is entirely at your own risk.

All copyrights are owned by their owners, unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

You are strongly recommended to take a backup of your system before major installation and backups at regular intervals.

1.3 Credits

In this version I have the pleasure of acknowledging

```
Dustin Webber (@mephux) and Wes Garrison
```

Any comments or suggestions can be mailed to doncicuto [at] gmail.com

2. Installation. First steps.

2.1 Update your list of packages and install some debian packages

```
# apt-get update
# apt-get install unzip ruby1.9.1 ruby1.9.1-dev build-essential libxslt1-dev
libpng12-dev libjpeg62-dev ttf-dejavu libtiff4-dev libjasper-dev libfontconfig1-
dev libxml2-dev ghostscript libopenexr-dev libwmf-dev librsvg2-dev libfftw3-dev
liblzma-dev liblcms1-dev graphviz-dev libdjvulibre-dev openssl xorg libssl-dev
mysql-server mysql-client libmysqlclient-dev
```

2.2 Install Java from Oracle web page

Maybe it's not needed, but one of the ruby gems complains with a warning if Java is not installed.

```
# wget http://download.oracle.com/otn-pub/java/jdk/7u1-b08/jdk-7u1-linux-
i586.tar.gz
# tar xvf jdk-7u1-linux-i586.tar.gz
# mkdir /usr/java
# mv /usr/local/src/jdk1.7.0_01 /usr/java/latest
# update-alternatives --install /usr/bin/java java /usr/java/latest/jre/bin/java
20000
# update-alternatives --install /usr/bin/javaws javaws
/usr/java/latest/jre/bin/javaws 20000
# update-alternatives --install /usr/bin/javac javac /usr/java/latest/bin/javac
20000
# update-alternatives --install /usr/bin/jar jar /usr/java/latest/bin/jar 20000
```

2.3 Installing rubygems

```
# cd /usr/local/src
# wget http://production.cf.rubygems.org/rubygems/rubygems-1.8.10.tgz
# tar xvfz rubygems-1.8.10.tgz
# cd rubygems-1.8.10/
# ruby1.9.1 setup.rb
# cd ..
```

2.4 Installing ImageMagick

ImageMagick version must be >= 6.6.4, so let's compile it.

```
# wget ftp://ftp.sunet.se/pub/multimedia/graphics/ImageMagick/ImageMagick-6.6.9-
7.tar.gz
# tar xfz ImageMagick-6.6.9-7.tar.gz
# cd ImageMagick-6.6.9-7/
# ./configure
# make && make install
# cd ..
```

2.5 Installing wkhtmltopdf

```
# wget http://wkhtmltopdf.googlecode.com/files/wkhtmltopdf-0.11.0_rc1-static-
i386.tar.bz2
# tar xvjf wkhtmltopdf-0.11.0_rc1-static-i386.tar.bz2
# mv wkhtmltopdf-i386 /usr/local/bin/wkhtmltopdf
# chmod +x /usr/local/bin/wkhtmltopdf
# cd ..
```

2.6 Installing rails and other ruby gems needed

```
# gem1.9.1 install rails
# gem1.9.1 install bundler
# gem1.9.1 install pdfkit
```

3. Installing Snorby

3.1 Get Snorby

First of all, get Snorby at snorby.org.

```
# unzip Snorby-snorby-v2.3.10-0-ga1b1e28.zip
# cd Snorby-snorby-a1b1e28/
```

3.2 Modify the configuration files

Modify the user and password for your mysql server

```
# vi config/database.yml
```

Set the ip address and port in the test section e.g domain: x.x.x.x:3000

```
# vi config/snorby_config.yml
```

3.3 Install Snorby

```
# bundle install
# bundle exec rake snorby:setup
```

3.4 Test it!

```
# rails server -e test
```

Go to http://x.x.x.x:3000. Are you seeing this?
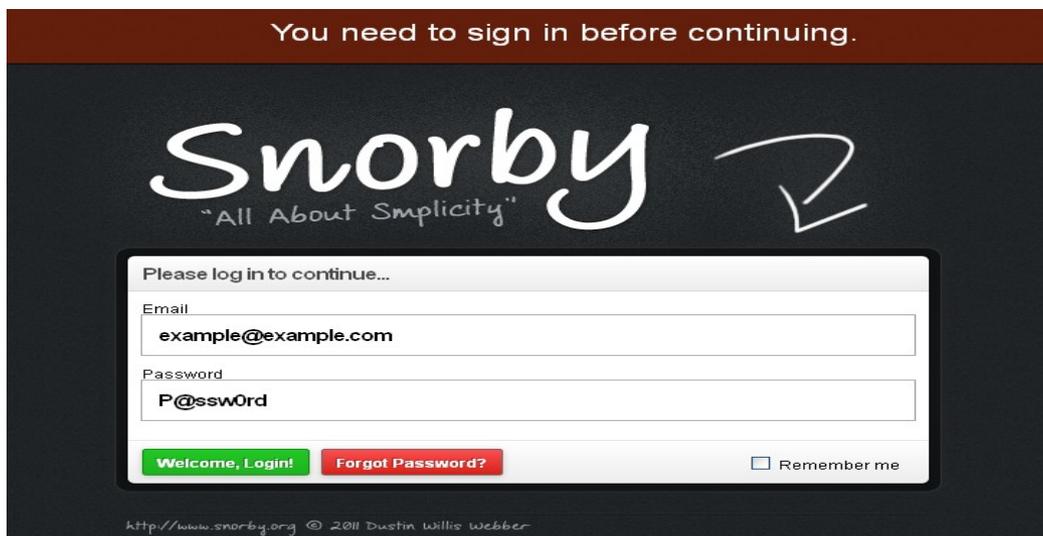
Authenticate yourself with snorby@snorby.org and the password snorby

Congratulations!

New chapters about configuration will be added soon.

Please *contact me* if you have found any *errors* or any *questions*