



BlackHole: Installation and Configuration Manual.

Nicolas Rebagliati

Guide to install and configure BlackHole.

Index

Index	2
Overview:	3
Installation:	5
Configuration:	7
Configuration of folders:	7
Database Configuration:	8
Web Server Configuration:	9
Application Configuration:	10
Administrative Users:	10
Environment:	11
Host:	11
User Identity:	12
Session Identity:	12
Profile:	13
Private Key:	14
User:	15
Usage:	17
Chat:	19
Web:	20
Extras:	22
Known Bugs:	23

Overview:

Blackhole was designed to solve a problem we had where I work.

Our problem was that we had a very large server platform, and a large number of users needing to connect to them. Mostly to give support.

Furthermore users are constantly modified, thus had two choices.

Create all users on all servers (were too many) or we created a generic user for all of them.

The first option was impractical, especially for the high rotation of users.

And the second was clearly unsafe, because there was no way to keep trace to each user or where it was connected to.

We needed something that was easy to manage and give us visibility of what users did.

How it works?

Blackhole primarily a frontend, all users connection should be via this server.

And the application is configured as user shell, to be the only thing they can run.

The database contains the information of all servers, grouped by environments.

Then there are the private keys to be used for each connection depending on the user.

Then each user has a profile associated with the servers that each user is allowed to connect.

The application is a curses-menu with the list of enabled servers.

Which contains all servers to which we have permission to connect.

But much more than that because blackhole stores information for each connection established.

- What user
- The user used to connect
- Time of login
- Time logout
- Connection duration
- The use (the number of commands that run / connect time)
- The amount of keypresses

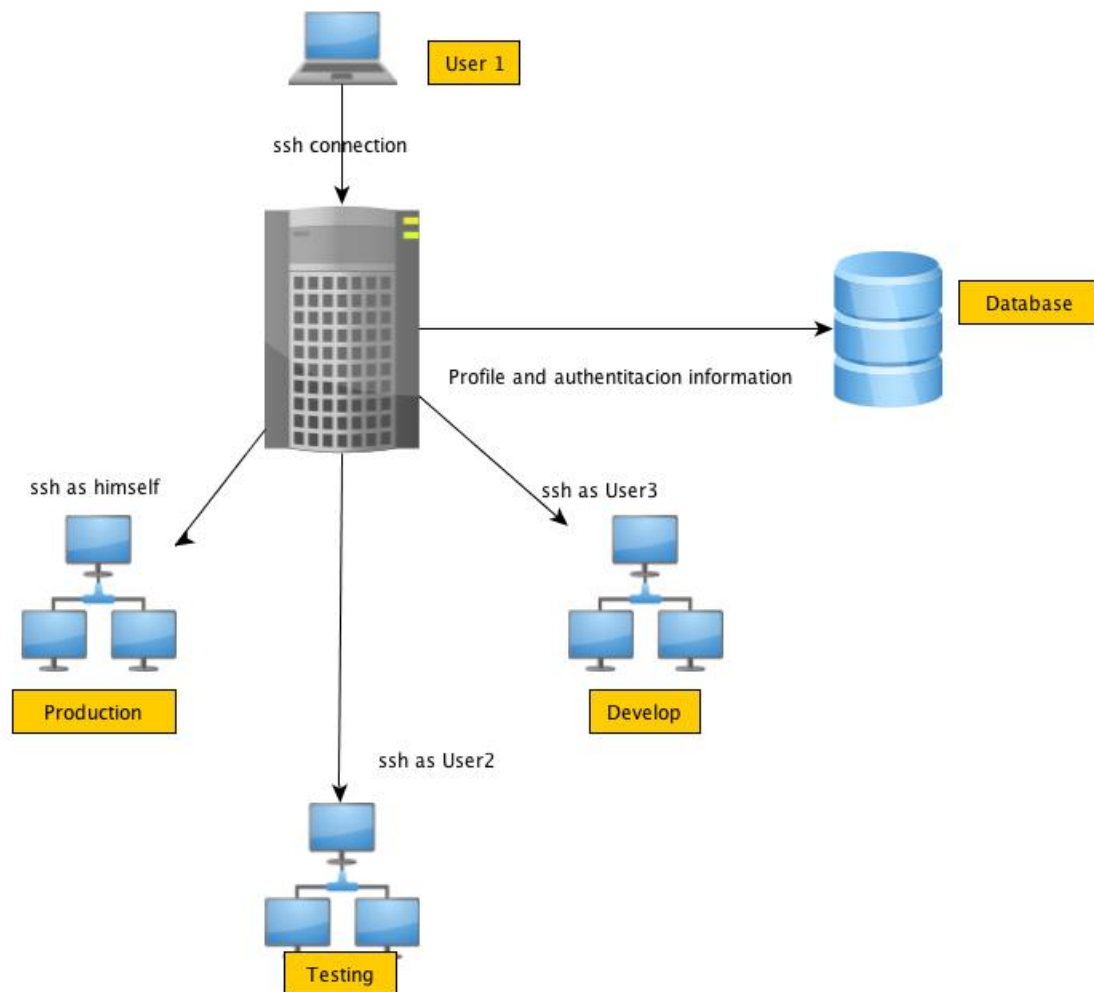
But also keeps a log of all the contents of each connection.

All this information can be viewed from the web that is integrated, which allows us to generate graphics and download the log for each connection.

Functionality Extras:

Apart from the above, Blackhole has other functionalities.

- Chat server, where users can talk online.
- Validation by token, can optionally enable token validation (which is sent by mail), and until it is entered correctly the user can not access.
- Enabling user by time range, or a small group of servers.



Installation:

The installation process is a bit complex, since it has several dependencies.

The application is written in python and is based on the Django framework.

It runs on Linux (tested), OSX (tested) or any other UNIX compliant units.

This manual is a fresh install.

The installation was done on a Linux (Ubuntu 12.04) with LAMP (Apache-MySQL-PHP), Django 1.4 (was developed and tested with this version, although it might work with less. But I do not know), python 2.7 (with 2.6 should work fine).

First of all, install all dependencies.

- Django (<https://www.djangoproject.com/>)
- paramiko
- MySQLdb
- Urwid
- python-simplejson
- django-qstats-magic
- python-dateutil
- django_extensions
- libapache2-mod-wsgi (Only if you want to use apache)

Most can be installed via apt.

I recommend install Django using the tarball in their website.

apt-get install python-mysqldb python-paramiko python-urwid python-simplejson libapache2-mod-wsgi

There are three that we use pip (Python Package Index):

pip install django-qstats-magic python-dateutil django_extensions smplib

With this done, we need to create the database and a user. (For this there are no instructions, I recommend installing phpmyadmin and do it from there).

This manual will use a database called blackhole, with a username and password blackhole / blackhole.

I recommend using a more secure password in production.

The next step is to install the application.

As the application runs as Shell users, we will install in the / home. But it may be where you want:

cd /home

tar zxvf BlackHole.tgz

We must create a group (eg blackhole), which must be the primary group of all users who use the application.

groupadd blackhole

Now it is very important to change the permissions.

```
cd /home/blackHole  
chown -R root:blackhole ./
```

Configuration:

Configuration of folders:

The next step is the configuration, the first thing to do is modify the configuration file named `blackhole.config` located in `/home/BlackHole/`

This is the content

```
[settings]
debug = False
application_path = /home/BlackHole
log_path = /home/BlackHole/logs
chat_enabled = True
token_validation_enabled = False
```

`APPLICATION_PATH` value must be equal to where the application installed.

And `log_path` entry is the directory where we want to keep logs of the sessions.

It is very important to make sure that directory is writable for the group `blackhole`.

NOTE: the logs will be stored in this directory, but will first try to be written in a directory with the name of the user profile within this directory. If that directory does not exist, will be stored in the directory indicated by `log_path`. These directory must be created by hand, and must also have write permissions for the group `blackhole`.

Here is also set if we want to enable chat option, and the option of token.

Enabling token found here is global, then you can enable each user.

Database Configuration:

Once you have created the database and the user.

We have to enter it in the file: `/home/BlackHole/black_hole/settings.py`

In "DATABASES", we enter:

- "NAME": the name of the database created
- "USER": the name of the user created
- "PASSWORD" user password set

NOTE: In addition to this we can change the TimeZone file.

Example: `TIME_ZONE = 'America / Chicago'`

And the language. Example: `LANGUAGE_CODE = 'en-us'`

Currently the only enabled languages are English (en-us) and Spanish from Argentina (es-AR).

Once it is ready, we need to create the tables.

For this we have to run the following command:

```
cd /home/BlackHole
```

```
./manage.py syncdb
```

and then to load some necessary settings:

```
./manage.py initial_setup
```


Web Server Configuration:

To run the website integrated with blackhole have 2 options.

Run it with apache, or run it through the webserver built with django (Which is not recommended).

To facilitate integration with apache, delivered two necessary configuration files.

They are in "/ home / BlackHole / apache"

In django.wsgi only must modify the installation directory is different from the manual.

Copy the file site.example to the directory sites-available, and you must enable it (if you modify the installation directory, must also be modified in this file):

```
site.example cp / etc/apache2/sites-available/blackhole
```

```
a2ensite blackhole
```

In the configuration file example uses port 8080, so we have to enable the port in apache adding this to / etc/apache2/ports.conf

```
NameVirtualHost *: 8080
```

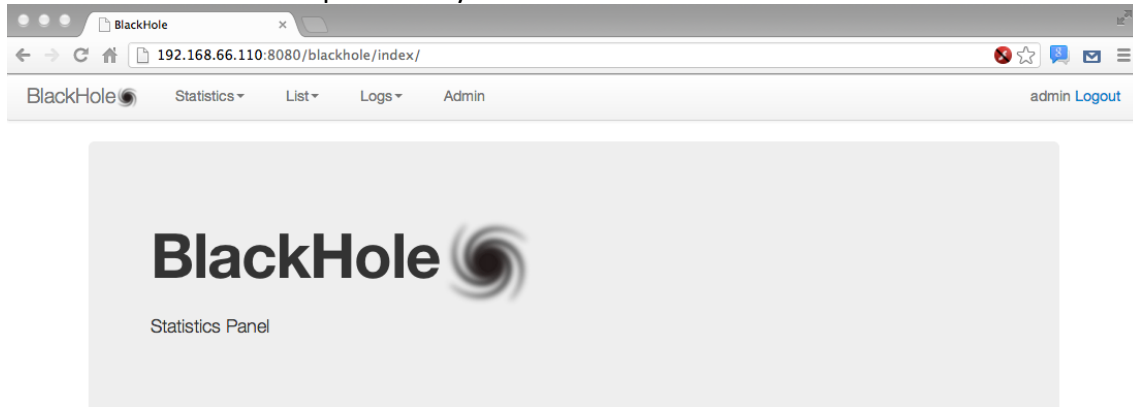
```
Listen 8080
```

We can restart the apache.

We enter it through this url:

<http://localhost:8000/blackhole/index/>

With the username and password you created earlier to create the database.



Application Configuration:

Now should load all the information about the user, servers, etc. keys.

By clicking on the "Admin", take us to this page:

BlackHole Administration

Site administration

Auth		
Groups	+ Add	✎ Change
Users	+ Add	✎ Change
Black_Hole_Db		
Environments	+ Add	✎ Change
Hosts	+ Add	✎ Change
Private Keys	+ Add	✎ Change
Profiles	+ Add	✎ Change
Session Identities	+ Add	✎ Change
Session Logs	+ Add	✎ Change
User Identities	+ Add	✎ Change
Users	+ Add	✎ Change

We must make a distinction between "Auth-> Users" and "Black_Hole_Db-> Users".

In the first option the user must be created that will manage the application only.

The second are the users who will be using it.

Likewise you can create groups for administrative users who can do specific tasks.

Such as enabling and disabling users, but only that.

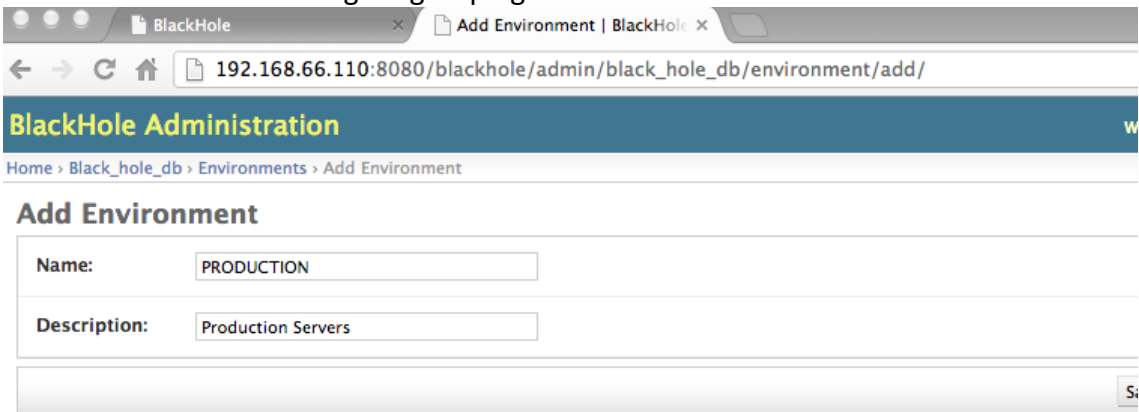
Administrative Users:

In Auth-> Users, we create these administrative users. Remember that for these users can access this site must be on the "Staff".

If you do not want to use groups, and just need that the users can so anything. Instead of giving specific permissions, they can enable as "Superuser".

Environment:

The environments are a logical grouping of servers.

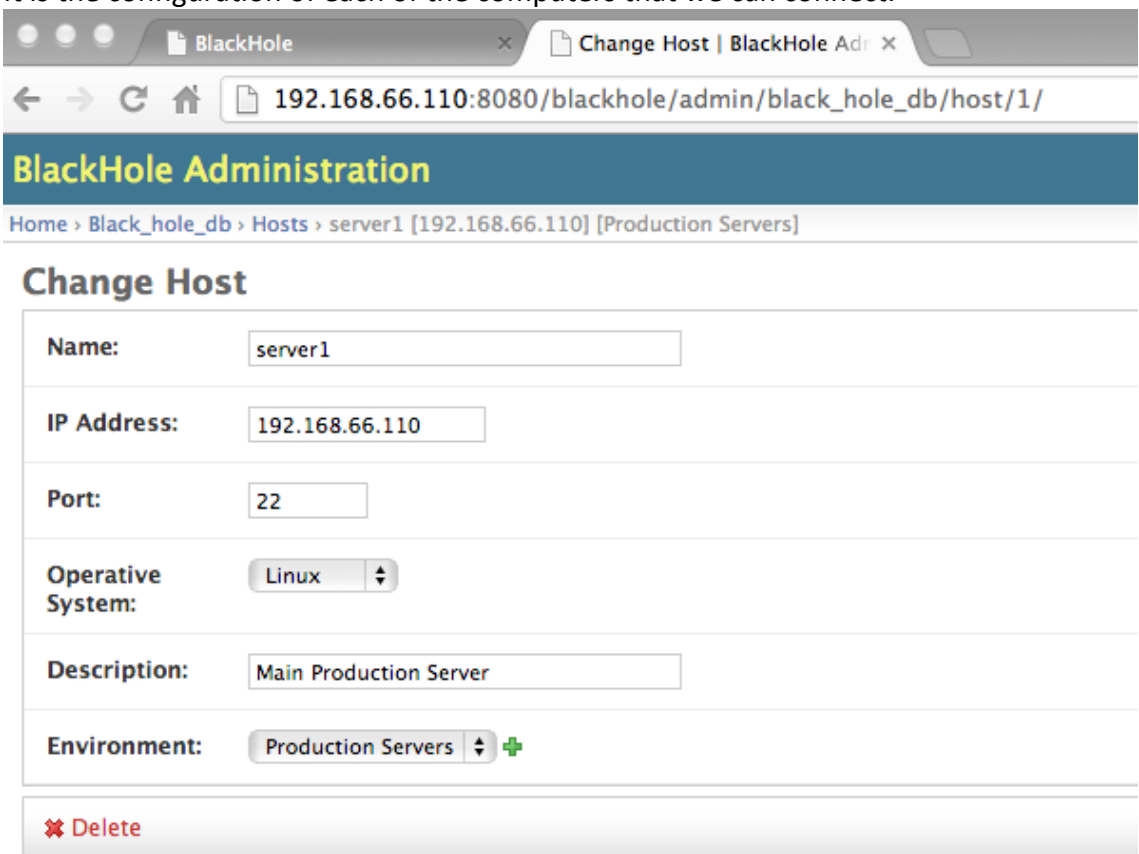


The screenshot shows a web browser window with the address bar displaying `192.168.66.110:8080/blackhole/admin/black_hole_db/environment/add/`. The page title is "BlackHole Administration". The breadcrumb trail is "Home > Black_hole_db > Environments > Add Environment". The main heading is "Add Environment". Below this, there are two input fields: "Name:" with the value "PRODUCTION" and "Description:" with the value "Production Servers". At the bottom right, there is a "Save" button.

NOTE: Do not use spaces in the Name field, since it is used for directories of logs and can cause problems.

Host:

It is the configuration of each of the computers that we can connect.



The screenshot shows a web browser window with the address bar displaying `192.168.66.110:8080/blackhole/admin/black_hole_db/host/1/`. The page title is "BlackHole Administration". The breadcrumb trail is "Home > Black_hole_db > Hosts > server1 [192.168.66.110] [Production Servers]". The main heading is "Change Host". Below this, there are several input fields and a dropdown menu: "Name:" with the value "server1", "IP Address:" with the value "192.168.66.110", "Port:" with the value "22", "Operative System:" with a dropdown menu showing "Linux", "Description:" with the value "Main Production Server", and "Environment:" with a dropdown menu showing "Production Servers" and a green plus icon. At the bottom left, there is a "Delete" button with a red X icon.

User Identity:

The user identity is a fundamental concept that must be understood well.

The user identity is the user who will be using to connect to the selected device.

By default identity is created called "self".

Identities to be created are generic users.

For example if you have users connecting users with their own personal, they will use the identity "self".

Example, if we have a user named John and he must connected to server A as the user John, for that he will have to connect as "self".

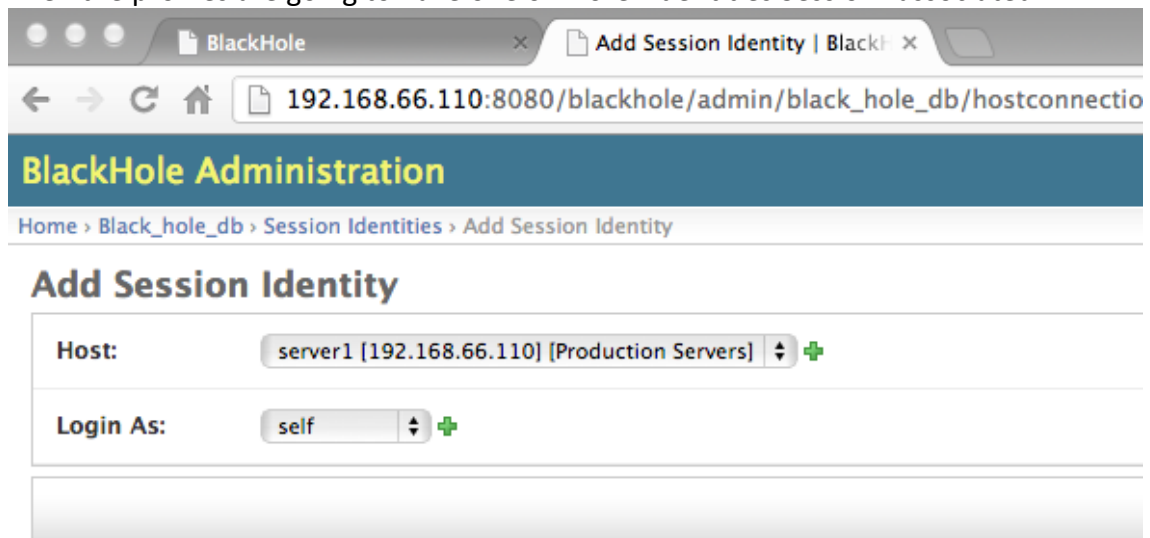
But if that same user on server B is connected as the admin user for that server will have to connect with the identity "admin".

And that must be created here, but not the identity John.

Session Identity:

The session identity is another important concept is going to associate a user identity to a server.

Then the profiles are going to have one or more "Identities Session" associated.



The screenshot shows a web browser window with the address bar displaying `192.168.66.110:8080/blackhole/admin/black_hole_db/hostconnectio`. The page title is "BlackHole Administration". The breadcrumb navigation is `Home > Black_hole_db > Session Identities > Add Session Identity`. The main heading is "Add Session Identity". Below this, there are two form fields: "Host:" with a dropdown menu showing "server1 [192.168.66.110] [Production Servers]" and a green plus icon, and "Login As:" with a dropdown menu showing "self" and a green plus icon.

Profile:

Here we create different user profiles.

The profiles are a group of Session Identities, you cant have 2 Session Identities to the same host in one profile (See Known Bugs).

The screenshot shows a web browser window with the address bar displaying `192.168.66.110:8080/blackhole/admin/black_hole_db/profile/add/`. The page title is "BlackHole Administration" and the breadcrumb trail is "Home > Black_hole_db > Profiles > Add Profile".

The main heading is "Add Profile". Below it, there is a form with the following fields:

- Name:** A text input field containing the value "TEST".
- Hosts:** A section for selecting hosts. It includes a note: "Hold down 'Control', or 'Command' on a Mac, to select more than one." Below this note is a list titled "Available Hosts" with a search filter input. Below the available hosts is a list titled "Chosen Hosts" which contains two entries:
 - server1 [192.168.66.110] [Production Servers] as self
 - stan [192.168.66.102] [Testing Servers] as aenima

Private Key:

Private keys are the means used to connect to servers.

The private keys are by environment, so for our servers in the same environment we have loaded the same public keys for a user to be connected to one or more servers that environment.

One important thing is that you take should be created this way.

Example if I have two Session Identities :

- John -> server1 (PRODUCTION) -> as self
- John -> server2 (PRODUCTION) -> as admin

So I have 2 keys created

One for the user admin and one for the user john (both for the PRODUCTION environment).

It is very important to select the correct type of key (DSA or RSA).

The screenshot shows the 'Add Private Key' page in the BlackHole Administration interface. The browser address bar shows the URL: 192.168.66.110:8080/blackhole/admin/black_hole_db/privatekey/add/. The page title is 'BlackHole Administration'. The breadcrumb trail is 'Home > Black_hole_db > Private Keys > Add Private Key'. The form contains the following fields:

- User:** aenima
- Environment:** Testing Servers (with a dropdown arrow and a plus icon)
- Key Type:** DSA Key (with a dropdown arrow)
- Private Key:** A text box containing a DSA private key, starting with '-----BEGIN DSA PRIVATE KEY-----' and ending with '-----END DSA PRIVATE KEY-----'.
- Public Key:** A text box containing an ssh-dss public key, starting with 'ssh-dss' and ending with '-----END DSA PRIVATE KEY-----'.

A 'Save' button is located at the bottom right of the form.

User:

The user has several fields that are optional, and are only useful if you use some extra functionality of BlackHole, as is the token validation.

The screenshot shows the 'Change User' page in the BlackHole web interface. The browser address bar shows the URL: 192.168.66.110:8080/blackhole/admin/black_hole_db/user/1/. The form contains the following fields and options:

- User:** nrebagli
- Name:** Nicolas
- LastName:** Rebagliati
- Email:** test@test.com
- Identifier:** 1234
- Profile:** TEST (with a dropdown arrow and a plus icon)
- ☒ **Enabled**
- ☒ **Log Session**
- ☐ **Enabled in Time Range**
- Since:** 12:34:00 (with 'Now' and a clock icon)
- To:** 12:34:00 (with 'Now' and a clock icon)
- Enabled Environments:**
 - Available Enabled Environments (with a search filter): Production Servers, Testing Servers
 - Chosen Enabled Environments (empty)
 - Buttons: Choose all, Remove all
- Last Login:**
 - Date: (empty) (with 'Today' and a calendar icon)
 - Time: (empty) (with 'Now' and a clock icon)
- ☐ **Generate Token**
- Celular Phone:** (empty)

The email field is not mandatory, but if you want to use email token must be complete.

The identifier field is some type of identifier of the user. But it is not mandatory.

When a user is disabled, you can not connect to any server.

But there is another option, which is to enable it in a time range, and if outside this range can not enter any server.

For this option to work, the user has to be enabled.

Since that option is evaluated before this.

Also can be restricted to environments that can log in, in this way even though the user has permissions to access other servers, it will not be able to connect.

Mobile field is to post token via SMS. Not required.

And finally the Log Session option is to disable any user on time to avoid saving your sessions files (but will be stored in the database for statistics).

Usage:

When everything is ready, users will connect by ssh to blackhole and this would provide them the options they have available.

```
1. nrebagli@blackhole: /home/BlackHole (ssh)
root@blackhole: /home/Bl... nrebagli@blackhole: /hom... bash bash
BlackHole (v4.0) User: Rebagliati, Nicolas [nrebagli] - Selected: Testing Servers
[-] Production Servers Hosts: 1
    server1 - Main Production Server
[-] Testing Servers Hosts: 1
    stan - Testing Server

Move: up,down,home,end,left,w/Mouse Expand: space,click Select: enter,DoubleClick Quit: q
Chat: c By: Nicolas Rebagliati [nicolas.rebagliati@aenima-x.com.ar]
```

The movement can be done with the keyboard or mouse.

When a user completes its ssh connection, select the server that is going to be taken back to this menu.

1 BlackHole: Installation and Configuration Manual.

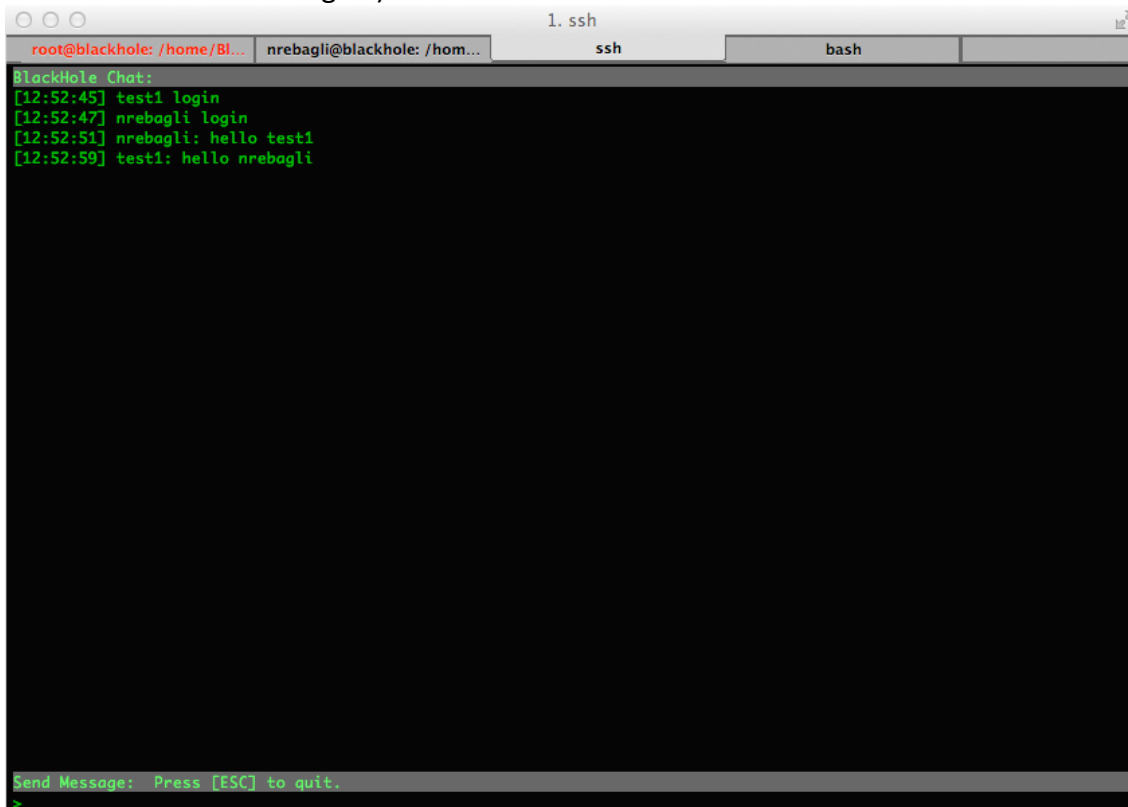
If you have any problems with any keys when connected, will be indicated to the user.

```
1. ssh
root@blackhole: /home/Bl... nrebagli@blackhole: /hom... ssh bash
BlackHole (v4.0) User: Test, User [test1] - Selected: Testing Server
[-] Production Servers Hosts: 1
  server1 - Main Production Server [Private Key Missing or Invalid Format]
[-] Testing Servers Hosts: 1
  stan - Testing Server

Move: up,down,home,end,left,w/Mouse Expand: space,click Select: enter,DoubleClick Quit: q
Chat: c By: Nicolas Rebagliati [nicolas.rebagliati@aenima-x.com.ar]
```

Chat:

If the option is enabled users can chat with to each other with the option in the menu (the user can log in once, if you already have another open chat connection, you will not be able to connect again).

A screenshot of a terminal window titled "1. ssh". The terminal shows a chat session in BlackHole. The chat log displays the following messages: [12:52:45] test1 login, [12:52:47] nrebagli login, [12:52:51] nrebagli: hello test1, and [12:52:59] test1: hello nrebagli. At the bottom of the terminal, there is a prompt "Send Message: Press [ESC] to quit." followed by a green cursor. The terminal window has tabs for "root@blackhole: /home/BI...", "nrebagli@blackhole: /hom...", "ssh", and "bash".

```
root@blackhole: /home/BI... nrebagli@blackhole: /hom... ssh bash
BlackHole Chat:
[12:52:45] test1 login
[12:52:47] nrebagli login
[12:52:51] nrebagli: hello test1
[12:52:59] test1: hello nrebagli

Send Message: Press [ESC] to quit.
>
```

The Chatserver process must be running to use this functionality.

cd /home/BlackHole

nohup ./startChatServer.py &

Web:

In statistics we find many statistics, which can be requested by user or server.

User:

Test, User [test1]

From:

05/11/2012

To:

November 2012

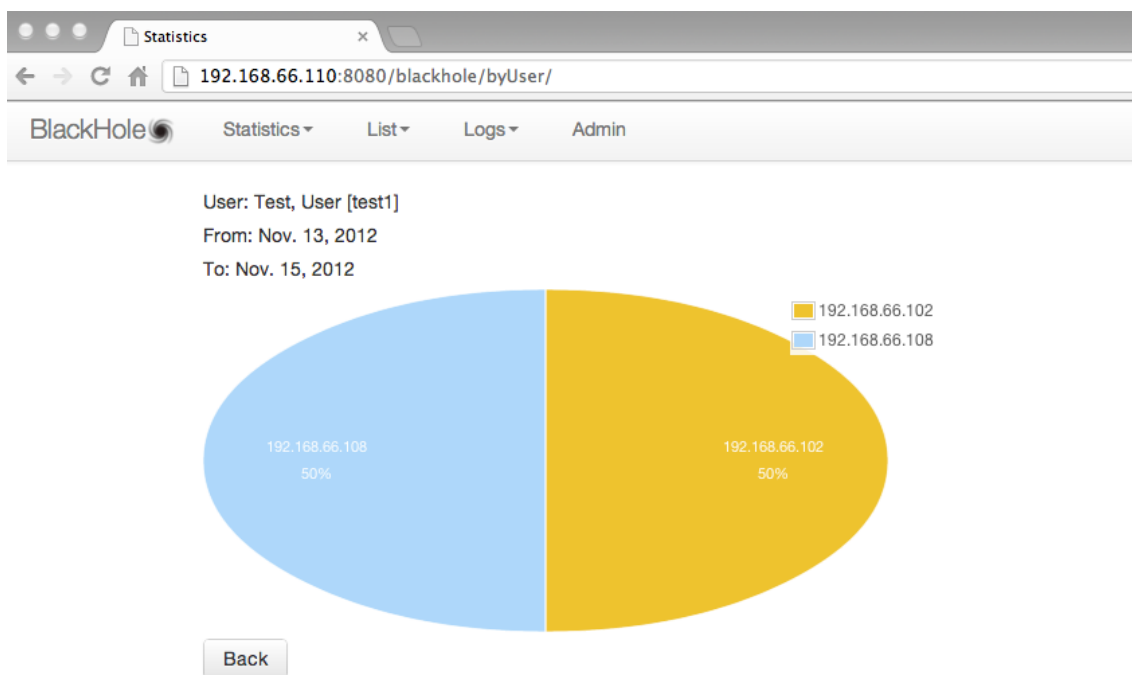
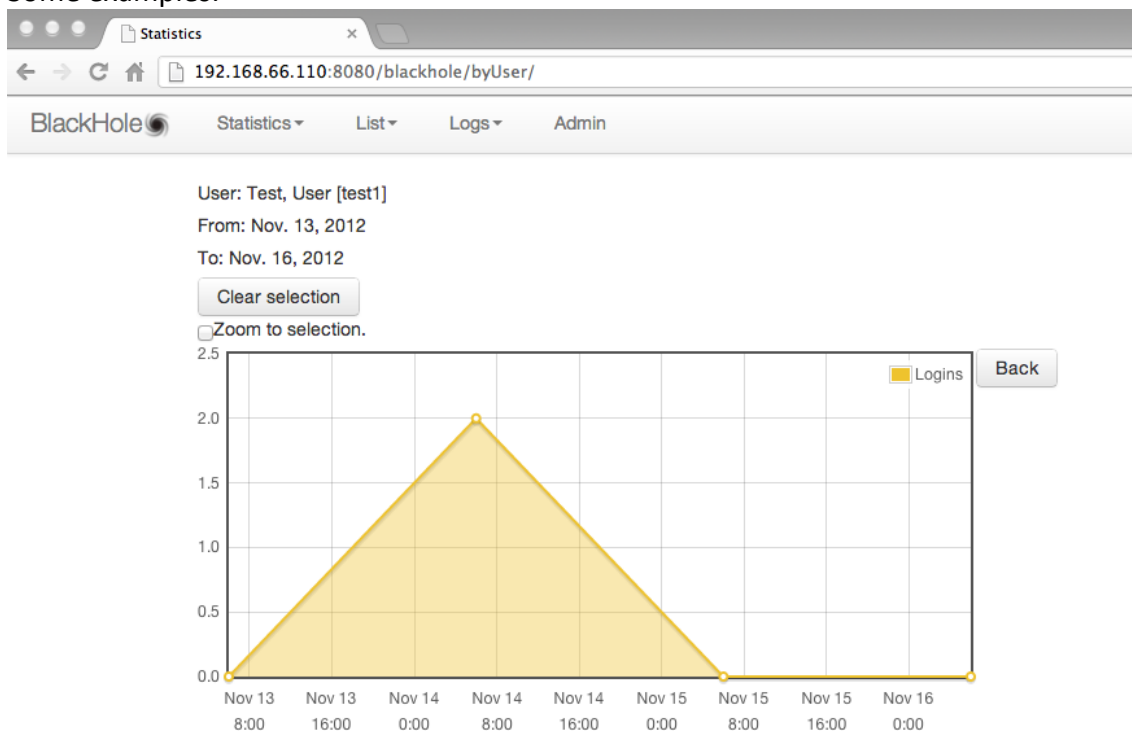
Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

For each one we can select a time range and a statistic type.

In option logs we can find the option to search for a particular user sessions in a time range and then you can download the log of each session.

SessionID	User	Host	Login as	Source IP	Login Date	Logout Date	Blackhole Server	Download
404299	test1	stan	aenima	192.168.66.102	Nov. 14, 2012, 1:09 p.m.	Nov. 14, 2012, 1:09 p.m.	blackhole	Download

Some examples:



Extras:

As I wrote before, there are some extra features that are not enabled.

- Validation of the web by radius (see notes in settings.py)
- Toek sent by mail, in addition to enable it in the configuration file you must modify the credentials in `/home/BlackHole/black_hole_gui/emailSender.py`
- Token can also be send by SMS, but you need to have access to a SMSC. If you want that you need to change the configuration in `/home/BlackHole/black_hole_gui/smsSender.py`

You can send me an email if you have questions about these.

Known Bugs:

There are still several things to fix, the main ones are:

- You can not put in a profile 2 Identities session of the same host. Blackhole but will have a problem in generating the menu and this will behave strangely. If you need a user can connect to the same server as 2 different users what we must do is create that host two times with different names and create 2 session identities.
- The size of the terminal when you connect from blackhole to a server is the same of you blackhole terminal. If we change the size before you connect to a server would fit well, but if we change the window size after you connected to the server the terminal continue to have its original size.
- If the server that runs Blackhole is not very powerful, can be that when we have many users connected and run any command that writes a lot on screen (Example "run a select * from table"), it may be that others feel that this slow. This is because is consuming many resources to write on the screen and in the log of the session. Therefore it is recommended not to run it in virtual machine if you expect to have many users.