

Sguil Configuration and Installation

Sguil Version 0.5.3

15 January 2005

Note: If you decide to install Sguil, the Shadow sensor cronjob and startup in the /etc/rc.d/rc.local will be disabled. If you want to run both packet collection packages, which collect the same information, it can be enabled in both files previously mentioned.

Additional information available at: <http://sguil.sourceforge.net>

Installing Sguil with MySQL database.....	2
Installing Sguil without MySQL.....	2
Installing Sguil Database Server Only.....	2
Client Configuration	2
Sguil sguil.conf update.....	3
Client Access to Database.....	3
Setting up the database and its users.....	4
Change the mysql root password	4
Configuring Sguil Daemon	4
Adding a New User to Sguil	5
Removing a User from Sguil	5
Configure Snort Portscan.....	5
Configuring Barnyard.....	6
Configuring Sancp	6
Configuring Sensor Agent	6
Configuring Log Packets	7

Installing Sguil with MySQL database

```
mount /mnt/cdrom
cd /mnt/cdrom/sguil
run pkgtool
Select Current          Install packages from the current directory
                          Install the package located in this directory
```

Installing Sguil without MySQL

This package is for distributed sensors. On PC contains Sguil with MySQL database and the sensors report to it.

```
mount /mnt/cdrom
cd /mnt/cdrom/sensguil
run pkgtool
Select Current          Install packages from the current directory
                          Install the package located in this directory
```

Installing Sguil Database Server Only

This package is for distributed sensors. On PC contains Sguil with MySQL database and the sensors report to it.

```
mount /mnt/cdrom
cd /mnt/cdrom/sguildb
run pkgtool
Select Current          Install packages from the current directory
                          Install the package located in this directory
```

Client Configuration

Download the Windows Sguil client at:

http://sourceforge.net/project/showfiles.php?group_id=71220

Unpack in C:\sguil-0.5.3

Download Windows Active TCL at: <http://www.activestate.com/Products/ActiveTcl/>

Install at c:\tcl

Download Windows TLS libraries at: <http://tls.sourceforge.net>

Unpack in C:\tcl\lib

Download Ethereal for Windows at: <http://www.ethereal.com>

Install at C:\Ethereal

Download Firefox for Windows at: <http://www.mozilla.org/>
Install at C:\Firefox

Sguil sguil.conf update

Edit c:\sguil-0.5.2\client\sguil.conf

```
# Change SERVERHOST to the correct IP or servername  
set SERVERHOST 192.168.30.4
```

```
# Set up OpenSSL here (read ./doc/OPENSSL.README)  
# 0=off 1=on  
set OPENSSL 1
```

```
# win32 example  
set ETHEREAL_PATH "c:/ethereal/ethereal.exe"
```

```
# win32 example (IE)  
set BROWSER_PATH "c:/firefox/firefox.exe"
```

```
# Display a GMT clock in the upper righthand corner  
# 1=on 0=off  
set GMTLOCK 1
```

```
# Mailserver to use for emailing alerts  
set MAILSERVER mail.example.com
```

```
# Default From: address for emailing  
set EMAIL_FROM foo@example.com
```

Install Ethereal and Firefox as shown as it will greatly simplify configuring the sguil.conf file as the path will all be DOS 8.3 filename compliant. The TLS libraries are used to encrypt the session between the Windows client and the database server.

Client Access to Database

The client can access the database at this point by executing the sguil.tk. However, sguil.tk must be associated with the “wish application” before it will start.

c:\sguil-0.5.2\client\sguil.tk

Setting up the database and its users

If mysql database is not started, start it this way:

```
/usr/local/mysql/bin/mysqld_safe user=mysql --bind-address=127.0.0.1 &
```

Change the mysql root password

By default, the MySQL database is started to **listen to 127.0.0.1 only** via the startup script which will prevent external connections to TCP port 3306. However, the mysql database default password is blank (no password assigned) and must be changed immediately with the following command:

```
/usr/local/mysql/bin/mysqladmin -u root password 'your-new-password-for-sql_user-root'
```

The default Sguil password is **password**. If all of the components are running on the same computer or you use Stunnel to encrypt the data between the sensor and database (seen stunnel.pdf in the release note on the CD), it can be left as password since the database can only be access via 127.0.0.1. However, if you wish to change the password, it can be changed with the following command or you can use the Webmin administrative tool but remember it must be changed as well where indicated in this document (where the sguil account is used).

```
mysql -p (root password set earlier)
\u mysql (User mysql)
```

```
GRANT ALL ON sguildb.* TO sguil@127.0.0.1 IDENTIFIED BY \
'make_a_password_for_user_snort' WITH GRANT OPTION;
\q (Quit mysql)
```

Note: When entering the passwords for the sguil user, ensure it gets enclosed in single quotes or you will get an error.

Configuring Sguil Daemon

Creating your own SSL client/server certificate.

There is already in place a default SSL certificate but you can create your own using the script supplied in the root account. To create your own client/server certificate, execute the following script:

```
/root/sguil_certificate
```

Follow the directions to create your own personal certificate. This certificate is used to encrypt communication between the console and the server.

If you are running all of the components on the same box, these settings will work immediately. If you previously changed the sguil password in the previous section, change any of the following according to your new setup (i.e. password):

```
cd /etc/sguild  
vi sguild.conf
```

```
set DBNAME sguildb  
set DBPASS password  
set DBHOST 127.0.0.1  
set DBPORT 3306  
set DBUSER sguil
```

Adding a New User to Sguil

Add a user to login the Sguil database via the client after this setup has been completed. To add a new user do:

```
/etc/sguild/sguild –adduser guy [Enter]  
Enter your password and verify
```

Removing a User from Sguil

Add a user to login the Sguil database via the client after this setup has been completed. To add a new user do:

```
/etc/sguild/sguild –delduser guy [Enter]
```

Configure Snort Portscan

```
/cd /usr/local/snort/etc  
vi snort.external.conf
```

```
Find: preprocessor portscan-ignorehosts: $HOME_NET
```

This line is used to ignore host or range of hosts that trigger the portscan preprocessor. You may need to modify this later.

```
Find: preprocessor portscan: $HOME_NET 4 3 /LOG/external/portscans shadow
```

Change **shadow** to the hostname of the sensor

Configuring Barnyard

You can uncomment the default settings for Barnyard to start logging. However, if you change the user and password to for logging into the database, you will need to edit the barnyard.eth1.conf file to change the settings:

```
cd /usr/local/barnyard/etc
```

```
edit barnyard.eth1.conf
```

Find: config hostname: **shadow** (Change shadow to the correct sensor name)

(Go to the bottom with Shift-G)

Uncomment the following two lines (#)

```
output sguil: mysql, sensor_id 0, database sguildb, server 127.0.0.1, user sguil, \
password password, sguil_host 127.0.0.1, sguil_port 7736
```

Note: If your server is something other than **127.0.0.1**, change it accordingly.

Configuring Sancp

This package is preconfigured on the sensor and does not require immediate changes.

```
vi /etc/sancp/sancp.conf
```

This is the configuration file for sancp. By default it will work but if you would like to exclude some stuff, it can be done in here.

sancp is started by the /etc/rc.d/sancpd_eth1 script

Configuring Sensor Agent

This agent connects the sensor to the Sguil console. It enables the analyst to request additional information from the sensor (traffic stream, Ethereal pull, etc).

```
cd /usr/local/sguil/bin
vi sensor_agent_eth1.conf
```

Find: set SERVER_HOST **127.0.0.1**

Only change localhost if the SERVER_HOST if the database is on a remote host. If the installation is on the same system, it can remain this way.

Find: set HOSTNAME **shadow**

Change **shadow** to the correct sensor hostname.

Configuring Log Packets

This script is used to collect packets by the sensor to be accessed later by the sensor_agent. Those files are used to do further analysis on the events collected by the Snort sensor.

```
cd /usr/local/sguil/bin  
vi log_packets_eth1.sh
```

Find: HOSTNAME=”**shadow**”

Change **shadow** to the correct sensor hostname.