# Plesk

# qsheff, Clamav Virrenscanner, Plesk 8.2

http://www.enderunix.org/qsheff/

# wget http://www.enderunix.org/qsheff/qsheff-II-2.1.tar.gz

# tar -zxf qsheff-II-2.1.tar.gz
# cd qsheff-II-2.1

Clamav:
Install the Debian packages clamav, clamav-daemon and clamav-freshclam libclamav-dev

plesk:~# apt-get install clamav clamav-daemon clamav-freshclam libclamav-dev

Download and extract qsheff and ripmime tar balls.

plesk:~# cd /usr/local/src/
plesk:/usr/local/src# wget http://www.enderunix.org/qsheff/qsheff-II-2.1.tar.gz
plesk:/usr/local/src# wget http://www.pldaniels.com/ripmime/ripmime-1.4.0.5.tar.gz
plesk:/usr/local/src# tar zxvf qsheff-1.0-r4.tar.gz
plesk:/usr/local/src# tar zxvf ripmime-1.4.0.5.tar.gz

Building and installing ripmime is straightforward:

plesk:/usr/local/src# cd ripmime-1.4.0.5
plesk:/usr/local/src/ripmime-1.4.0.5# make
plesk:/usr/local/src/ripmime-1.4.0.5# make install
Ripmime will now be installed in /usr/local/bin; an appropriate place, and right where
qsheff expects it.

To see installing options:

```
# ./configure --help
  --enable-debug              Enable debug messages
  --disable-local-users       Disable the filters for local users
  --enable-syslog             Enable syslog messages
  --enable-backup             Enable backup
  --enable-spam-tag           Enable Spam Tagging
  --enable-virus-tag          Enable virus tagging
  --enable-custom-error       Enable the custom error patch
  --enable-qq-patch           Enable qmailqueue patch

  --with-max-bodyline         Maximum number of lines to filter, default=40
  --with-maxfiles             Maximum numbers of files in a dir.
  --with-qmailgroup           Define qmail group, default=qmail
  --with-qmaildir             Define qmail directory, default=/var/qmail
  --with-clamav               Enable ClamAv
  --with-clamd-socket         Path to clamd socket, default=/tmp/clamd
```

--with-custom-prog Enable User Defined Program, check qsheff.conf

You can you any of these options.

A typical installation should be like this:

```
# ./configure --disable-local-users --with-clamav \
   --with-clamd-socket=/var/run/clamav/clamd

./configure \
--enable-debug \
--with-clamav \
--with-clamd-socket=/var/run/clamav/clamd.ctl \
--enable-syslog \
--enable-backup \
--enable-spam-tag \
--enable-virus-tag

./configure --enable-debug --with-clamav --with-clamd-socket=/var/run/clamav/clamd.ctl --enable-syslog --enable-backup --enable-spam-tag --enable-virus-tag
```

Options are described below. Installing should continue like this:

```
# make && make install
# /usr/local/etc/qsheff-II/install-wrapper.sh
```

After installing, /var/qmail/bin folder shoul be seen like:

```
-r-s--x--x  1 root    qmail  36766 17 May 16:57 qmail-qsheff
lrwxr-xr-x  1 root    qmail     27 16 May 15:28 qmail-queue -> qmail-qsheff
-r-s--x--x  1 qmailq  qmail  12396  2 May 15:43 qmail-queue.orig
```

Options:

--enable-debug Enable debug messages
Used for printing debugging information to screen in case of any problem

--disable-local-users Disable the filters for local users
qSheff filters local users by default. Bu small corporations does not need this. This option deactivates this feature.

--enable-syslog Enable syslog messages
Logging information is sent both to qsheff.log and to syslog. With this option, logs can be stored in a remote syslog server.

--enable-backup Enable backup
Enables logging all incoming/outgoing e-mail traffic

--enable-spam-tag Enable Spam Tagging
Instead of rejecting spammed e-mails, qSheff tags subject and delivers e-mail to user. Users can store these e-mails in a seperate folder by writing their own rules in client side.

--enable-virus-tag Enable virus tagging
Infected e-mail is delivered to user after replacing content with a warning text about the virus. This message is predefined as VIRI_CENSOED in src/main.h. custom_sign in qsheff.conf is appended to this message automatically.

--enable-custom-error Enable the custom error patch
By default, qmail responds to users with "permanently error" in the case of spam or virus. Usually this response does not have much information. Bu option enables custom-error patch. But qmail should be patched with this patch before. Predefined messages are in src/main.h like DEFAULTMSG, SPAMMSG and VIRUSMSG. Messages are tagged with "SPAM" keyword or name of the virus automatically.

--enable-qq-patch Enable qmailqueue patch
Enables qmail-queue patch. This patch should be applied before. More information is described in Chapter 3 WORKING PRINCIPLES. With this option, qSheff is triggered through QMAILQUEUE environment variable, not symbolic link. This environment variable usually assigned in /etc/tcp.smtp

--with-max-bodyline Maximum number of lines to filter, default=40
Limits maximum number of lines in an e-mail to filter. Predefined value is 40. This option is a countermeasure for DOS attacks which can be caused by sending very large e-mails. Spam words usually appear in first 10 lines. It's not needed to scan all of the body.

--with-maxfiles Maximum numbers of files in a dir.
if --enable-backup is activated, qSheff logs all e-mail traffic. Every OS has limit for number of file entries in a folder. If this option is defined, qSheff will switch to next folder afterwards. qSheff assumes 32000 by default.

--with-qmailgroup Define qmail group, default=qmail
if qmail is installed with a group id other than "qmail", should be specified here

--with-qmaildir Define qmail directory, default=/var/qmail
If qmail is installed other than /var/qmail, should be specified here.

--with-clamav Enable ClamAv
Activates ClamAv antivirus software. If ClamAv is installed to nonstandart folder like /opt/clamav, this folder should be specifed here. Otherwise, ClamAv library functions will fail during make.

--with-clamd-socket Path to clamd socket, default=/tmp/clamd

qSheff connects to ClamAv daemon directly throug UNIX socket. Path to socket should be specified here if different than /tmp/clamd. Another solution is changing LocalSocket variable to "/tmp/clamd" from clamd.conf

--with-custom-prog Enable User Defined Program, check
User can make qSheff run any program or script. 3rd party software, anti-virus programs or your own scripts can be run this way. Full path to program/script and parameters is given as parameter. Internal variables can be passed to custom program like %%mailfrom%%, %%mailto%%, %%remoteip%%,
%%msgfile%% ve %%tempdir%%. This parameters or path to program can be changed within qsheff.conf later.

6. CONFIGURATION

qSheff configuration files are placed in etc/qsheff-II under install directory

qsheff.conf:

QSHEFFDIR: qSheff folder. Contaions backup, quarantine, spool and tmp folders.
LOGFILE: Specifies the file which qSheff will write logs to.
RIPMIME: Specifies full path to ripmime binary. Automatically detected and written by qSheff in configure process.
debug_level: Logging level. Default value is 99 and logs everything. If you set 14, then HEADER debugging informations will not be logged.

| | |
|---|---|
| 0 | ERR |
| 2 | QUEUE |
| 3 | VIRUS |
| 5 | CUSTOM |
| 11 | SPAM |
| 13 | ATTACH |
| 15 | HEADER |

enable_blackhole: If set to 1, no response will be sent to sender of the mail in case of error, spam or virus
paronia_level: Not yet implemented
drop_empty_from: If set to 1, qSheff rejects mails without a "From:" header.
enable_quarantine: If set to 1, spam or infected mails are quarantined.
enable_ignore_list: If set to 1, does not filter the mail addresses and ip addresses in ignore list
enable_header_filter: If set to 1, header filter is activated
enable_body_filter: If set to 1, body filter is activated
enable_attach_filter: If set to 1, attachment filter is activated
enable_clamd: If set to 1, ClamAv virus checking is activated
enable_custom_prog: If set to 1, running custom program is activated.
CUSTOM_PROG: Spesifies the full path and parameters of custom program.
CUSTOM_RET_MIN: The minimum return value of custom program in case of a match
CUSTOM_RET_MAX: The maximum return value of custom program in case of a match

For example a custom prog which returns 5 for virus and returns 9 for spam can be set with 5 as CUSTOM_RET_MIN and 9 as CUSTOM_RET_MAX
CUSTOM_RET_ERR: Value which custom program returns in case of error.
custom_sign: When virus tagging is enabled, this message is appended to the warning mail. Can be company logo/signature. This message is also contaions the information message which will be sent to user when "custom error" patch is applied.
qsheff.attach: The list which attachment filter looks for matching
qsheff.ignore: The list of e-mail and ip addresses which will not be filtered Regular expressions can be written. qSheff will try to match expressions with remote side IP and sender email address.
qsheff.rules: Contains qSheff spesific rules. Rules beginning with "h" are header rules. Rules in the same line like (rule1)(rule2) are operated with logic AND and rules in different lines are operated with logic OR.

7. USAGE

After installing qSheff, log file should be examined in order to be sure that everything is fine.

# tail -f /var/log/qsheff.log
04/05/2006 19:12:39: [qSheff] SPAM, queue=q1146759159-792935-50066, relayfrom=
88.247.172.183, from=`simsek@enderunix.org', to=`simsek@acikakademi.com', subj
=`viagra', size=575, spam=`Subject: viagra', rule=`(Subject:)([vV]iagra)'

17/05/2006 16:59:50: [qSheff] VIRUS, queue=q1147899588-883933-43385, recvfrom=
83.26.32.122, from=`olago@neostrada.pl', to=`biwi@turx.com', subj=`Re: Merry Christmas!', size=19082, virus=`Worm.Zafi.D',

17/05/2006 17:03:39: [qSheff] HEADER, queue=q1147899819-136265-43522, recvfrom=
84.50.27.182, from=`', to=`', subj=`', size=0,,

If filtering local users is deactivated, attempts from server will not be logged in log file.

If drop_empty_from=1 is set, attempts without "From:" line will be rejected and logged with HEADER tag.

If there is an error after qSheff delivers mail to qmail-queue, qmail-queue's exit value will be logged as exitcode.

17/05/2006 16:24:51: [qSheff] QUEUE, queue=q1147897465-631231-42376, recvfrom=
83.17.118.150, from=`edhzovsc@queretaro.com',
to=`alii@linuxxproggramlama.com',

# Plesk

subj=`Fw[36]: Hi !..', size=10240, error=`', exitcode=54

Eindeutige ID: #1031
Verfasser: Michael Stender
Letzte Änderung: 2009-03-19 04:37