



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Open Source Qmail-Scanner for Qmail MTA

Yongman Suh

February 4, 2002

Introduction

In the beginning of 1999, *I-Worm/Happy99* has appeared in the wild. On May 2000, there was an epidemic of *VBS/Love_letter* in the Internet. Now, the worm/virus issue hold an important position in security area. Recently, various worms including *Win32/Nimda*, *Win32/Sircam.worm* and *Code_Red* have been widely spread over the Internet through email systems. Since email is a popular and efficient medium for communication between people, recent worms/viruses are spread over the globe by utilizing those email systems. By doing so, a virus or worm is able to infect huge number of email systems all over the globe within a few hours. Various mutations and copycats of the virus/worm could be created and spread within a few hours, also.

To prevent computers from the virus/worm infection, most companies use desktop anti-viral software. However, most anti-viral software can not solve the all virus/worm issues since most of them are utilizing signature-driven detection/prevention techniques and have difficulties in handling for the new breed of virus/worm efficiently. Moreover, most viruses/worms are spreading itself by creating a infected message and sending it to all email addresses within the email system.

To complement some limitations of those anti-viral software, a few vendors have released commercial solutions, called mail gateway, for MS Exchange and Lotus Notes. The intention of such solutions is to detect/remove virus/worm within email messages before they are delivered to end users. Unfortunately, no commercial solution is yet available for UNIX mail system.

Qmail-scanner is a freeware tool for Qmail MTA(Mail Transfer Agent), which scan/remove viruses from an email message. This article explores how to install and use Qmail-Scanner for UNIX and, also, shows an example which can be applicable in the working environment.

Freeware Scanning Tool

Qmail-Scanner

■ About Qmail-scanner

Qmail-Scanner is an open-source software, add on that enables a Mail Server to scan all incoming/outgoing Email based on attachment types (e.g. *.vbs, *.pif etc) or Email with certain Email headers (e.g. “**Subject:ILOVEYOU**” etc). Sometimes, it can be used in interface between Qmail and commercial virus scanning utilities. The latest release is version 1.01. You may get the latest release at SourceForge (<http://sourceforge.net>). It runs for only Qmail MTA, unfortunately.

■ Features

Jason Harr describes the following Qmail-scanner’s features on the “Qmail-Scanner:Email Scanning Harness for Qmail”.

- Works with any commercial Unix-based virus scanning utilities. (e.g. Trend’s Virus scanner, Sophos’s “sweep” virus scanner, H+BE DV’s antivir scanner, Kaspersky’s AVPLinux scanner, MacAfee’s virus scanner, F-Secure Anti-Virus scanner, InocuLAN Anti-Virus scanner)
- Can pick up viruses for which commercial scanning utility updates are not yet released.
- Can block Email based on particular attachment extensions or certain strings contained in headers.
- Adds a new **Received:** header with a virus report showing whether it is clean or not, and optionally add a descriptive header : **X-Qmail-Scanner** for user to know that a scanner is running on this Email Server.
- Supports English, Italian, German, Spanish, Turkish, Lithuanian, French and Chinese messages currently.
- Can log information of all messages which pass through the email system to “syslog” or an arbitrary file, debugging outputs to “/var/spool/qmailscan/qmail-queue.log”, and virus reports to “/var/spool/qmailscan/quarantine”.
- Supports Email encoded with the following schemes: MIME, uuencoded, TNEF along with ordinary ASCII text.

- Unpacks each message before running the scanners over it. It can also scan the original Email message as well as the unpacked messages. [1]

■ System Requirements

- **Qmail-Scanner-1.01** is available at <http://qmail-scanner.sourceforge.net/>
- **Qmail 1.03** is available at <http://www.qmail.org/>
- **reformime** from **Maildrop 0.73 or 1.1+** (Don't use 1.0, which has a major bug) is a part of the package.
(<http://www.flounder.net/~mrsam/maildrop/maildrop>)
- **Perl 5.005_03+**
- Perl module **Time::HiRes**
(<http://search.cpan.org/serch?module=Time::HiRes>)
- Perl module **DB_File** (most distributions come with it pre -installed)
(http://search.cpan.org/serch?module=DB_File)
- Mark Simpson's **TNEF unpacker** which decodes those annoying MS -TNEF MIME attachments that Microsoft mail servers helpfully use to encapsulate your already MIME encoded attachments.
(<http://world.std.com/~damned/software.html>)

■ Patches

Qmail-Scanner uses **qmail-scanner-queue.pl** script instead of original Qmail's **qmail-queue** binary. So you have to patch Bruce Guenter's **QMAILQUEUE** patch to enable Qmail MTA to work with Qmail -Scanner in proper. After the patch is done successfully, when a message comes, **qmail-scanner-queue.pl** runs firstly then it calls the original **qmail-queue** binary to toss the message. Note that there is a way to install without **QMAILQUEUE** patch at <http://qmail-scanner.sourceforge.net/manual-install.php>, and for Linux systems, a **patched qmail-1.03 RPM** is available at <http://untroubled.org/qmail+patches/>.

■ Installation Guide

1. Other packages

- Get all packages described in “**System Requirements**” section.
- Install **Perl 5.005_03+** and module **Time::HiRes** (and **DB_File** if not installed yet)
 - # rpm -Uvh perl-*
 - # perl -e 'use CPAN; install Time::HiRes '
- Install **Maldrop 0.73 or 1.1+**
 - # ./configure [options]
 - # make
 - # make install-strip
 - # make install-man
- Install **TNEF unpacker** (if necessary)
- Patch **QMAILQUEUE**
 - # tar xzvf qmail-1.03.tar.gz
 - # patch -p0 < qmailqueue-patch
- Install **Qmail 1.03** (see installation details at [Life with Qmail](#))
 - This is installed at “/var/qmail/” by default

2. Qmail-Scanner-1.01

- Check the permission of “suidperl” before Installation of Qmail -Scanner.
 - # ls -al /usr/bin/suidperl
 - # chmod 4710 /usr/bin/suid perl
- Install Qmail-Scanner
 - # ./configure --install

This command not only checks what package is installed on your system automatically, but also warns you which package should be pre -installed. So, you can install all needed packages previously.

When the installation is done, this will create directories (default path is “/var/spool/qmailscan”) and qmail-scanner-queue.pl (/var/qmail/bin/qmail-scanner-queue.pl) perl script.
- Modify Qmail startup scripts (e.g. /etc/rc.d/init.d/qmail) like below.
 - #!/bin/sh
 - QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
 - export QMAILAUEUE
 - ALIAS_UID='id -u alias'
 - ALIAS_GID='id -g alias'
 - exec /usr/local/bin/softlimit -m 2000000 \

```
/usr/local/bin/tcpserver -v -p -x/etc/tcp.smtp.cdb -u \  
$ALIAS_UID -g $ALIAS_GID 0 25 /var/qmail/bin/qmail-smtpd 2>&1
```

This script enables Qmail to know to use qmail -scanner-queue.pl instead of original qmail-queue. Note that you should set QMAILQUEUE variable as mentioned above and export it just before invoking qmail -smtpd.

- Configure quarantine -attachments.txt
Modify /var/spool/qmailscan/quarantine -attachments.txt file to block specific types of attachment extension or strings in headers. Here are some examples showing how to configure that file to ban specific Email.

- Strings in headers

<Format>

String<TAB>Header<TAB>Description of Virus

<Example> Sircam Worm

ILOVEYOU Virus-Subject: VBS/Love_Letter

Note that each file should be delimited by <TAB> and header must start with “**Virus-**” string.

- Attachment extensions

<Format>

Filename<TAB>Size (in b ytes)<TAB> Description of Virus

<Example>

.mp3 0 MP3 attachment disallowed

This would ban any Email containing MP3 attachments passing.

■ Test Installation

- Run ./contrib/test_installation.sh -doit
 - This will simply send an Email containing the **EICAR.COM** test virus to

"root". If your Qmail-Scanner installation is correct, this will result in the Email being blocked and your Qmail -Scanner administrator will receive an Email saying this has occurred. If not, check installation processes again.

- If Qmail-Scanner catches the infected Email, then it blocks and quarantines them to /var/spool/qmailscan/quarantine directory and sends alerting “Virus found” message to the Qmail -Scanner administrator.
- All events such as detecting an infected Email are logged in /var/spool/qmailscan/quarantine.log in a tab -delimited format.

■ Usage in Fields

We have used Qmail-Scanner 1.01 on our network since August 2nd, 2001 and set up this tools on Red hat Linux 6.2 (i.e. Linux 6.2 for Alpha CPU COMPAQ edition). Our Email Server has about 1,200 users and handles about 10,000 messages including all incoming/outgoing messages. However, there is no noticeable low efficiency.

For filtering Email, we added a particular string of header, which could block Sircam Worm, to the “/var/spool/qmailscan/qmail-attachment.txt” file such as: “**Multipart message<TAB>Virus-Content-Disposition:<TAB>Sircam.worm Virus**”. Surprisingly, it has caught **17,806** Emails compromised by Sircam Worm since the installation was completed.

It has some weak points, however. For example, if new viruses come in, we could not able to support proper headers to detect them immediately. However, an open society “[SorceForge](#)” on the internet was very helpful for various virus-related information. This site supports a number of mailing -lists for various viral issues including questions, suggestions and so forth. You, also, can get lots of tips about how to filter new coming viruses and other useful information, promptly.

A good way to protect internal PC ’s and servers of your organization from malicious Email viruses or worms is running a commercial virus scanning utility in parallel with Qmail-Scanner. Educating users to have awareness to the Email virus issues and to use a personal virus scanner properly is also very important. .

References:

- [1] Jason Harr. "Qmail-Scanner:Email Scanning Harness for Qmail ". Qmail-Scanner Home Page at SourceForge. September 2nd, 2001. URL: <http://qmail-scanner.sourceforge.net> (December 7th, 2001)
- [2] Kevin Swab. "SMTP Gateway Virus Filtering with Sendmail and AMaVIS ". SANS Information Security Reading Room. August 8th, 2001. URL: <http://www.sans.org/infosecFAQ/email/amavis.htm> (December 7th, 2001)
- [3] Dave sill. "Life with Qmail" September 19th, 2001. URL: <http://www.lifewithqmail.org/lwq.html> (December 7th, 2001)
- [4] Jason Harr. "Qmail-scanner-general Archives". URL: <http://www.geocrawler.com/lists/3/SourceForge/4041/0/> (December 7th, 2001)
- [5] CPAN – Comprehensive Perl Archive Network. URL: <http://www.cpan.org> (December 7th, 2001)

© SANS Institute 2000 - 2002, Author retains full rights.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor