



Exim  
&  
SpamAssassin

By: Alex Villegas

Simplify.



All trademarks used herein are the sole property of their respective owners.

Simplify.

# Alex Villegas

- »» cPanel: Level II Support Representative 06/2006  
Level III Advanced Tech 05/2007
- »» Bilingual: Spanish – Interest on Linguistics.

# Spam Attack !

From	Subject	Date	Size
<b>Now Give</b>	<b>Give United Online Our</b>	04/08/2007 08:17 AM	11 KB
<b><u>improve salesAlso</u></b>	<b><u>New degree of sexual confidence and control</u></b>	04/08/2007 04:42 PM	3 KB
<b><u>Ten</u></b>	<b><u>Elevate sex drive to new levels</u></b>	04/07/2007 07:13 PM	3 KB
<b><u>Chan Davis</u></b>	<b><u>VIAGR@ is the best thing I've ever had!</u></b>	04/06/2007 10:32 PM	14 KB
<b><u>Press</u></b>	<b><u>Loan for a low month payment</u></b>	04/06/2007 06:28 AM	3 KB
<b><u>Gambling Scenarios</u></b>	<b><u>She'll love your</u></b>	04/06/2007 09:21 AM	3 KB
<b><u>Phone Friend</u></b>	<b><u>- Lotto Tickets from 50 countries</u></b>	04/06/2007 07:17 AM	12 KB
<b><u>Hilary Baker</u></b>	<b><u>Prescription free top med brand\$</u></b>	04/06/2007 11:27 AM	13 KB
<b><u>Treasure Island</u></b>	<b><u>Good Credit or Not</u></b>	04/06/2007 05:14 PM	3 KB
<b><u>Rafael Fontenot</u></b>	<b><u>OEM XP Prof repair/reinstall over Action Pack XP Prof?</u></b>	05/06/2007 04:22 PM	24 KB

# Introduction

In this course we will be covering the following topics:

- »» Exim – cPanel's default mail server.
- »» SpamAssassin – Open Source Spam Filter.

Concentrating on their functionality, integration within cPanel as well as other methods to fight SPAM.

# About Exim

- Exim was written by Philip Hazel at the University of Cambridge in 1995. Still maintained by him.
- It was written using the basic philosophy of Smail\*.
- It's acronym was derived from “Experimental Internet Mailer” since the outcome of the project was unknown.
- Exim is Open Source and distributed under the GNU General Public License (GPL)

\*Note: Smail (a mail transport agent) is free software, but it is not a GNU package.

# Exim: Mail Transfer Agent

- Exim is defined as a Mail Transfer Agent (MTA)
- Mail User Agents (MUAs) refer to the program end users utilize to send and receive mail. They are commonly known as mail clients: **outlook, thunderbird**, etc.
- The core functions reside on the MTA, as the MUA simply sends the email to the MTA which then process the mail delivery from host to host until it reaches the proper destination.

# Sending E-mails - SMTP

- The Simple Transfer Protocol (SMTP) is used to send e-mails from host to host.
- By default it listens on port **25**. However it can be configured to use **26** as well.
- SMTP can also use a SSL implementation. Port **465** is reserved for SMTP over SSL.

# Sending E-mails - SMTP

## TLS

➤➤ Exim employs Transport Layer Security (TLS\*) in order to avoid utilizing an additional port for secure communications.

\*Note: With TLS, only a single service port is used which means no change to your current firewall or network set up is required to use TLS.

# E-mail Format – RFC 2822

- **RFC 2822** mandates the format of e-mail messages.
  - »» A message must contain a header and a body.
  - »» Headers have specific requirements and are terminated with a blank white line.

# E-mail Format – RFC 2822

➤➤ RFC permits the following address variations:

**user@domain.com**

Name LastName<**user@domain.com**>

**user@domain.com** (Name LastName)

Note: Anything within parenthesis is parsed as a comment.

# Exim Binary

»» Every Exim instance is independent and short lived.

- Exim main configuration is located at **`/etc/exim.conf`**
- Binary location: **`/usr/sbin/exim`**

It is important to state that on cPanel Servers sendmail is basically a symlink to the Exim binary, therefore all sendmail calls are processed by Exim.



# Custom Modifications

Custom modifications to `/etc/exim.conf` should be done using the **Advanced Exim Configuration Editor** in WHM to avoid them from been overwritten by the cPanel update.

Use RCS at the CLI to bypass the overwrite.

Simplify.

# Exim Routers

Exim mail delivery is handled by **3** types of drivers.

- The first type of driver is the **dnslookup router**. Basically Exim looks up the MX record for the domain and searches for an entry within the following file: **/etc/localdomains**, if existent the router is skipped.
- Remote mail servers **/etc/remotedomains**

# Exim Routers

Second type are defined as “**accept**” routers which state preconditions and are responsible for accepting ALL mail that passes the initial preconditions.

The most common use of this router is for setting up deliveries to local mailboxes. For example:

**localusers:**

**driver = accept**

**domains = mydomain.example**

**check\_local\_user**

**transport = local\_delivery**

# Exim Routers

The third level is called a “**redirect**” router which is basically responsible for filtering the e-mails.

The redirect router handles several kinds of address redirection. Its most common uses are for resolving local part aliases from a central alias file:

**`/etc/aliases`**

Note: SpamAssassin no longer works as a router but rather at the SMTP level.

# Exim Routers

The third level is called a “**redirect**” router which is basically responsible for filtering the e-mails.

The redirect router handles several kinds of address redirection. Its most common uses are for resolving local part aliases from a central alias file:

**`/etc/aliases`**

Note: SpamAssassin no longer works as a router but rather at the SMTP level.

# Exim Queue (1 of 2)

All messages that are handled by Exim are assigned their own **Message-ID**.

»» The syntax of such ID is 16 characters and separated into 3 parts by hyphens. Where each section is an encoded number using base 62.

First Section: **Unix time**

Second Section: **PID of the process**

Third Section: **Distinguish process from same PID and Unix Time.**

# Exim Queue (2 of 2)

»» The path to the Exim Queue is as follow:  
**`/var/spool/exim/input`**

»» Exim Queue is split into 62 subdirectories:  
**`[a-z], [A-Z],[0-9]`**

# Exim Commands

»» Checking the queue via the command line:

**exim -bp**

»» Checking the number of e-mails on the spool:

**exim -bpc**

»» Examine contents of a particular message:

**exim -Mvl 'MessageID'**

»» Flushing the queue:

**exim -qff -v**

# What is Eximstats?

Eximstats is a Perl script which parses logs and creates a MySQL database with Exim statistics.

- You can view the output via WHM, under the “**View Mail Statistics**” menu option.
- If you ever need to restart this service you can use the following command:
- ```
/scripts/restartsrv_eximstats
```

# Repairing Eximstats

Corrupted Database:

```
cd /var/lib/mysql/eximstats  
myisamchk *
```

```
db.opt sends.frm sends.MYD sends.MYI smtp.frm smtp.MYD smtp.MYI
```

# Exim Log Files

»» There are three major Exim log files that assist you monitor and troubleshoot:

Exim Main Log: `/var/log/exim_mainlog`

Exim Reject Log: `/var/log/exim_rejectlog`

Exim Panic Log: `/var/log/exim_paniclog`

Note: Some distributions such as FreeBSD keep the logs under the following directory `/var/log/exim`. The core OS mail file `/var/log/maillog` is also helpful for troubleshooting purposes.

# /var/log/exim\_mainlog

```
2007-04-25 19:38:42 1HgmO1-00025M-FU malware acl  
condition: clamd: unable to connect to UNIX socket  
/var/clamd (No such file or directory)
```

```
2007-04-25 19:37:10 1HgmMY-0001xb-2D => user@domain.com  
R=lookuphost T=remote_smtp H=mail-in.domain.com  
[192.168.1.1]
```

```
2007-04-25 19:37:10 1HgmMY-0001xb-2D Completed
```



# /var/log/exim\_rejectlog

X-AntiAbuse: ID = 80e8a8941009bcd5bf34f4a058c37dc2

**R Reply-To: user@yahoo.com**

**F From: "Dr.Anthony Hobson" <fakebigpimp@excite.com>**

MIME-Version: 1.0

**X-Sender: fakebigpimp@excite.com**

X-Mailer: PHP

Content-Type: text/plain; charset="us-ascii"

Content-Transfer-Encoding: 7bit

**I Message-Id: <20070425183915.79B622F669@any.anydomain.com>**

Date: Wed, 25 Apr 2007 14:39:15 -0400 (EDT)

2007-04-25 19:39:25 1HgmOi-00028X-Qr H=(wazmzo) [192.168.1.3]

**F=<fakebigpimp@excite.com> temporarily rejected after DATA**

Simplify.

# /var/log/exim\_paniclog

```
2007-04-25 19:43:10 1HgmSM-0002UI-AX malware acl  
condition: clamd: unable to connect to UNIX socket  
/var/clamd (No such file or directory)
```

```
2007-04-25 19:43:40 1HgmSo-0002Ve-T9 malware acl  
condition: clamd: unable to connect to UNIX socket  
/var/clamd (No such file or directory)
```

Note: If exim has any critical errors they will be logged in **exim\_paniclog**. Should generally be empty.



# Exim Basic Commands

Print a count of the messages in the queue:

```
exim -bpc
```

Print a listing of the messages in the queue (time queued, size, message-id, sender, recipient):

```
exim -bp
```

Print a summary of messages in the queue (count, volume, oldest, newest, domain, and totals):

```
exim -bp | exiqsumm
```



# Exim Basic Commands

Print what Exim is doing right now:

**exiwhat**

Display all of Exim's configuration settings:

**exim -bP**

**Would like to learn more commands?**

Simplify.



# More Exim Commands?

**RTFM**

(Read the “FINE” Manual)

**Man Page:**

<http://www.die.net/doc/linux/man/man8/exim.8.html>

Simplify.

# Maildir vs Mbox

»» Mbox – inbox, .trash

»» Maildir – cur, new, tmp

cPanel currently only supports **Maildir**.

We offer a conversion script: **/scripts/convert2maildir**

It provides you with the option to backup your mail.

»» Phone and ticket support assistance is offered if issues are experienced during the conversion.

»» For More Info:

<http://www.courier-mta.org/mbox-vs-maildir/>

**NOTE: NEOMAIL does not support Maildir.**

# Joke Break

## Audience:

Please share a joke!

Note: **Clean ones please.** Other sorts of jokes can be e-mailed to my personal e-mail account or discussed after hours.

# What is SPAM?

## DISCLAIMER

We will NOT be addressing the following kind of SPAM:

SPAM is a canned pork product made by the Hormel Foods

Corporation that has entered into folklore.

# What is SPAM?

- To indiscriminately send unsolicited, unwanted, irrelevant, or inappropriate messages, especially commercial advertising in mass quantities. Noun: electronic "junk mail".
- is **BULK Unsolicited E-mail**. The term spamming is also sometimes used by search engines to mean web sites that try to gain a higher listing by submitting hundreds of almost identical pages or by inserting hundreds of keywords within a web document.

# Is SPAM a big concern?

- »» In 2004 the California Legislature released a study that showed spam costs the US organizations more than \$10 billion.
- »» SPAM is not just a burden to the end user, it is also known to contain virus, trojans and spyware.
- »» Does cPanel offer any tools to combat SPAM:  
Yes, absolutely. It installs SpamAssassin by default as well as other resources that we will discuss.



# About SpamAssassin

Spam Assassin is an automated mail filter that uses a wide range of heuristic algorithms on mail headers and message body text to identify "SPAM" (**unsolicited bulk email**).

Once identified, the mail is tagged as "SPAM" for later filtering using the user's desktop mail client.

Simplify.



# SpamAssassin on cPanel 11

Exim now runs SpamAssassin scans @ smtp time in ACLS

Previously all mail coming into an account was scanned every time deliver was attempted. This was grossly inefficient.

The side affect of this is that if you have:

- \* Two domains WITH SEPARATE USERS
- \* SpamAssassin turned off on the first domain
- \* SpamAssassin turned on on the second domain
- \* Mail forwarded to an account on the second domain from the first domain

Simplify.



# SpamAssassin on cPanel 11

Any email that was sent to the first domain will be forwarded to the second domain unscanned as there is no SMTP session between the accounts as they are local.

Generally you just need to turn SpamAssassin ON for the other domain to solve the problem.

Simplify.



# Enabling SpamAssassin

- Enabling SpamAssassin globally:

**WHM -> Server Configuration -> Tweak Settings**

For more information, please visit the developer's website: <http://www.spamassassin.org/>

# Reinstalling SpamAssassin

➤➤ Reinstalling SpamAssassin:

```
/scripts/realperlinstaller --force Mail::SpamAssassin
```

# Testing SpamAssassin

»» Testing SpamAssassin (GTUBE):

<http://spamassassin.apache.org/gtube/>

**XJS\*C4JDBQADN1.NSBN3\*2IDNEN\*GTUBE-  
STANDARD-ANTI-UBE TEST-EMAIL\*C.34X**

# SpamBox

**SpamBox** is a utility that can be used combined with SpamAssassin that will allowed you to direct all of your SPAM email to an specific 'spam' folder rather than sending the e-mails to your main inbox.

» Enabling SpamBox is handled by accessing the cPanel interface under the SpamAssassin Menu.

**What if you forget to delete your SPAM folder contents?**



# New Account Level Filters

## cPanel -> Mail -> Account Level Filtering

Filter Name:

*The Filter name must be unique. If you give the filter the same name as another filter, it will be overwritten.*

### Rules

|                                   |                                     |                                  |                                  |
|-----------------------------------|-------------------------------------|----------------------------------|----------------------------------|
| <input type="text" value="From"/> | <input type="text" value="equals"/> | <input type="button" value="-"/> | <input type="button" value="+"/> |
|-----------------------------------|-------------------------------------|----------------------------------|----------------------------------|

### Actions

|                                              |                                  |                                  |
|----------------------------------------------|----------------------------------|----------------------------------|
| <input type="text" value="Discard Message"/> | <input type="button" value="-"/> | <input type="button" value="+"/> |
|----------------------------------------------|----------------------------------|----------------------------------|

Simplify.

# RBL's – Real Time Black List

- »» A Realtime Black List is a list of IP's that are known to allegedly house spammers on them or be owned by someone who allegedly harbors spammers.
- »» All emails coming from those IP's are blocked immediately.
- Examples of RBL's: **SPAMHAUS, SPAMCOP**



# SPAM Database Lookup

**DNSSTUFF.COM**

<http://www.dnsstuff.com/tools/ip4r.ch?ip=127.0.0.1>

**ROBTEX.COM**

<http://www.robtext.com/rbls.html>

Simplify.

# RBL's and Exim

Creating lsearch files. These files are used to manually block spammers, ignore certain domains or incoming hosts.

**`/etc/rblblacklist`**

**`/etc/rblbypass`**

**`/etc/rblwhitelist`**

Note: **`touch /etc/rblblacklist; touch /etc/rblbypass; touch /etc/rblwhitelist`**

# /etc/rblblacklist

Is a manual blacklist, it rejects specific spammer hosts  
BEFORE they can send more email to your server:

Syntax:

**anydomain.com**

**yourdomain.com**

**randomdomain.com**

# /etc/rblbypass

Bypasses RBL email testing for specific destination  
(local) domains that don't want RBL filtering:

Syntax:

**anydomain.com**

**yourdomain.com**

**randomdomain.com**

# /etc/rblwhitelist

Blocks RBL email testing for listed incoming hosts, (wildcards allowed), in case an important client's mailservr is listed on an RBL you use, also automatically excludes relayhosts:

Syntax:

**mail.anydomain.com**

**\*.yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyourdomain.com**



# RBL's and Exim Configuration

```
#!/# cPanel Exim 4 Config
```

Enter these lines:

```
domainlist rbl_blacklist = lsearch;/etc/rblblacklist
```

```
domainlist rbl_bypass = lsearch;/etc/rblbypass
```

```
hostlist rbl_whitelist = lsearch;/etc/relayhosts : partial-lsearch;/etc/rblwhitelist
```

\* RBL entries required in ACL Section as well as Router Section.

**HOWTO:** <http://www.webhostgear.com/175.html>

Simplify.

# Boxtrapper

- Boxtrapper basically uses the challenge response method to block email.
- All the e-mail that is not on the user configurable white list is held on a queue waiting for verification.
- The mail held on the queue will automatically get a response asking the sender of the address to verify the authenticity of the e-mail by replying to the message without modifying the header.
- E-mails with no valid ownership will get block.

# White & Black Lists

- You can use **`/etc/hosts.allow`** to whitelist remote mail servers.
- In addition you can use **`/etc/hosts.deny`** to black list mailservers.

**What if you want to do this via WHM?**

# White & Black Lists

## GUI Level:

➤➤ Main >> Security >> Security Center -> Host Access Control

For example, you could set up the following rules to lock down your SSH service:

| Daemon | Access List    | Action | Comment                         |
|--------|----------------|--------|---------------------------------|
| sshd   | 192.168.0.1/24 | allow  | Allow local SSH access          |
| sshd   | 198.66.254.254 | allow  | Allow SSH from my specific IP   |
| sshd   | ALL            | deny   | Deny access from all other IP's |

Note that the rules have an order of precedence. You need to place your allow rules before your deny rules if you are choosing to use the allow from a few, then deny from all technique.

# Eximmailtrap

**Eximmailtrap:** prevents illegal users from sending mail as it requires that them to be part of the **mailnull/mail group**.

»» Disabling eximmailtrap:

Remove **/etc/eximmailtrap**

Disable it on **/var/cpanel/cpanel.config**



# Sender Policy Framework

»» The Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery.

»» Exim supports SPF. Needs to be activated.

```
deny message = $sender_host_address is not allowed to send mail from  
$sender_address_domain  
spf = fail
```



# Sender Policy Framework

- An Example Policy: **John Doe** owns the domain **test.net**. He sends mail through his gmail e-mail account. Since he often receives bounces about messages he didn't send, he decides to publish an SPF record in order to reduce the abuse of his domain in e-mail envelopes:

```
test.net. TXT "v=spf1 mx a:blah.test.net  
include:gmail.com -all"
```

<http://www.openspf.org/>

Simplify.

# Domain Keys

»» DomainKeys is a Yahoo!-proposed system for verifying the domain of an e-mail sender. DomainKeys prevents forged e-mails from claiming to be from a domain it is not coming from.

»» Exim it is a DomainKey aware MTA.

Yahoo Domain Keys Documentation:

<http://antispam.yahoo.com/domainkeys>

# Other Filters

- Global: **`/etc/antivirus.exim`**

Used to block virus attachments (ie .exe).

- Domain Base: **`/etc/vfilter`**

It can be edited via the cPanel GUI interface:

**Cpanel-> Mail -> E-mail Filtering**

Exim Filter Documentation:

[http://www.exim.org/exim-html-4.50/doc/html/filter\\_toc.html](http://www.exim.org/exim-html-4.50/doc/html/filter_toc.html)

# Securing your Server

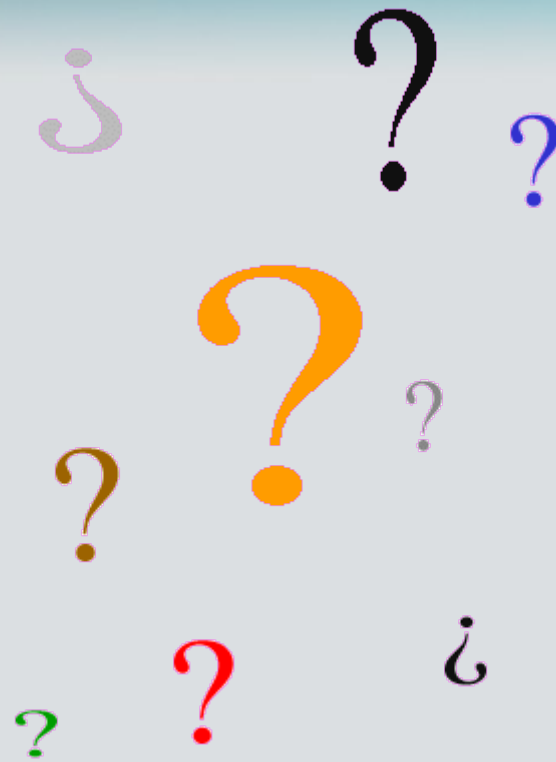
- Ensure that scripts running on your server are not vulnerable to spammers.
- Verify that the user “**nobody**” is unable to send out emails.
- Make sure your server is not an open relay\*:  
<http://www.abuse.net/relay.html>
- Enable **suExec** (perl/cgi scripts)
- Enable **phpSuExec** (php scripts)
- Adding **X-source headers** – Enable it on Tweak Settings

\* Note: An open mail relay is an SMTP (e-mail) server configured in such a way that it allows anyone on the Internet to relay (i.e. send) e-mail through it. cPanel by default prevents your server from being an open relay.

# POP QUIZ !!!

- 1.- What did you have for dinner?
- 2.- What is SpamAssassin?
- 3.- What does RBL stand for? Example of RBL?
- 4.- Does cPanel use Sendmail or Exim?
- 5.- Does cPanel support Maildir or Mbox?
- 6.- What are you doing tonight?

# Q & A



Simplify.