Protecting Linux Systems

By Govind Rammurthy – MD and CEO – MicroWorld Technologies Inc.

Due to its nature of open source code, Linux is fast becoming popular and is being deployed in ever increasing numbers on mail servers, corporate networks and desktops. Till recently, systems running on Linux were relatively free from virus and other threats. But with the greater penetration of Linux operating systems, virus authors have begun to target them.

This paper talks about threats faced by Linux mail servers and explains the recommended features that a good anti virus and anti Spam software should have.

Threats faced by Mail Servers

Mail servers are the workhorses and deliver mails on a 24x7 basis, until virus and other threats cripple them. This section discusses threats they face.

Spam

Spam is unsolicited junk mail sent to you or your mail server. People who indulge in such activities are called Spammers. These are sent by commercial advertisers who may offer dubious products, get rich schemes, products that do not suit your life style, promote illegal activities, etc. The intent here is to make you spend money. Almost 60% - to 70% of Spam is related to Porn. It costs the Spammer almost nothing to send mails and invariably get an eyeball count.

There is another type of spammer who sends large number of e-mails that flood your mailbox or mail server. The intent here is to cripple your e-mail service to such an extent that you cannot receive genuine mails. This is termed as Denial-of-Service (DOS) attack.

LOSSES CAUSED BY SPAM

Some of the losses caused by Spam are listed below:

- Spam is received through e-mails and may have alluring subject line like: Free offer, Chance of a lifetime, etc. Invariably you try to open the mail and read it. That is what the Spammer wants you to do. Opening the mail, reading it and then deleting it, consumes your Internet access time and costs you money. The mail servers that have delivered the mail through a series of servers have spent money and used bandwidth to deliver junk you did not want. Probably the junk mail was ahead in the queue for mails to be delivered and was given precedence over an urgent mail.

- Some Spam mails have attachments and the mail asks you to open it. If you do so, you risk running a virus that may be hidden in the mail. The costs involved in removing a virus from your system are massive.
- Some Spam mails after enclosing an alluring description of products or services, ask you to click on a link for further information. These links may open porn or other sites that you had no business visiting. But details of the visit are recorded in your server and you may have a lot of explaining to do.
- Products advertised through Spam mails require that you provide your credit card number and other personal information. Besides getting your account billed for junk items, you also open yourself to more Spam.

HOW SPAMMING IS DONE

There are many ways in which Spamming is done. The commonly used ones are: Rogue ISPs, One-Shot Accounts and Blind Relayers.

- **Rogue ISPs**: Spammers who have enough cash to fund their illegal activities run these. Rogue ISPs obtain their own network numbering and multiple domain names from the InterNIC. Spammers use multiple domain names and manage to get across Spam blocks. While it is possible to block a domain, it is not possible to block an ISP provider.
- '**On-the-fly' Spammers**: Such type of Spammers, register as multiple genuine users for trial accounts with ISPs. Forged identity or stolen credit cards are used to establish identities. They then use these accounts to start their Spam hits. By the time the ISP realizes that they are hosting a Spam run, the Spammer uses another account.
- **Blind Relayers**: Some innocent servers allow Blind Relaying – relaying messages without authentication. Spammers route their mails using these servers. The relay sends the mail and it appears as genuine.

Anti Virus

Mail servers run the double risk of getting infected by viruses and also transmitting them to other users. An infected mail server is very dangerous as it allows potential hackers a very easy means to attack other mail servers. They can be used to set up an infected P2P network. Viruses can spread at the rate of an epidemic. Infected mail servers need to be shut down and extensive clean up operations needed. Valuable mails could be lost resulting in huge potential losses.

Features of Anti Virus and Anti Spam Software

The ideal software uses a combination of Spam and Anti Virus and allow control over the mail server.

The following features are recommended in the Software:

Anti Spam Features

WHITE LISTS

The software should allow you to create a White List of clean domains and users. In addition there should be a list of 'Spam phrases'. Mails with such phrases should be blocked. The software should allow you to apply a severity level to the phrases from low to high. This allows you to control how Spam is identified.

Figure 1 shows a screen from MailScan for Linux, the top selling Anti Virus and Anti Spam software with features of White Lists and Spam Phrases.

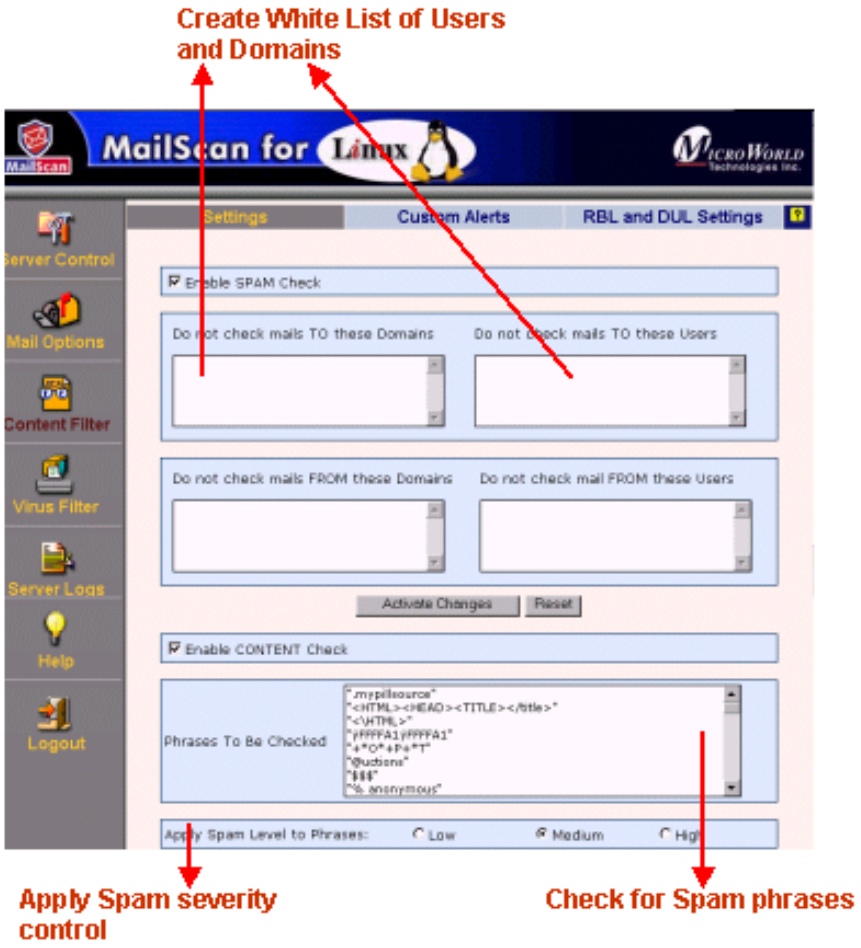

Figure 1. White Lists and Spam Phrases

RBL AND DUL CONTROLS

The software should have a list of RBL and DUL to verify a users authenticity.

MAPS (Mail Abuse Prevention System) provides a list of IP addresses that are known Spammers or allow spamming. This list is called as **Black hole list**. When your server, receives a mail from a domain, not on its allow domain list, you can send a query to MAPS Server which verifies the IP.

Spammers sometimes use stealth mail tactics when their initial Spam attempts are blocked. They use a **Dial-Up-Service** (DUL) provider to connect their Spam mail service, to the server. This is trespassing on your MailServer and the MAPS DUL project helps in identifying and stopping Spam. The project has a list of DUL users who are known Spammers. To verify if the request for connection to your Server is genuine, you can send a query to dialups.mail-abuse.org. The request is verified and returned.

Figure 2 shows a screen from MailScan for Linux, the top selling Anti-Virus and Spam software for Linux mail servers with features of RBL and DUL.

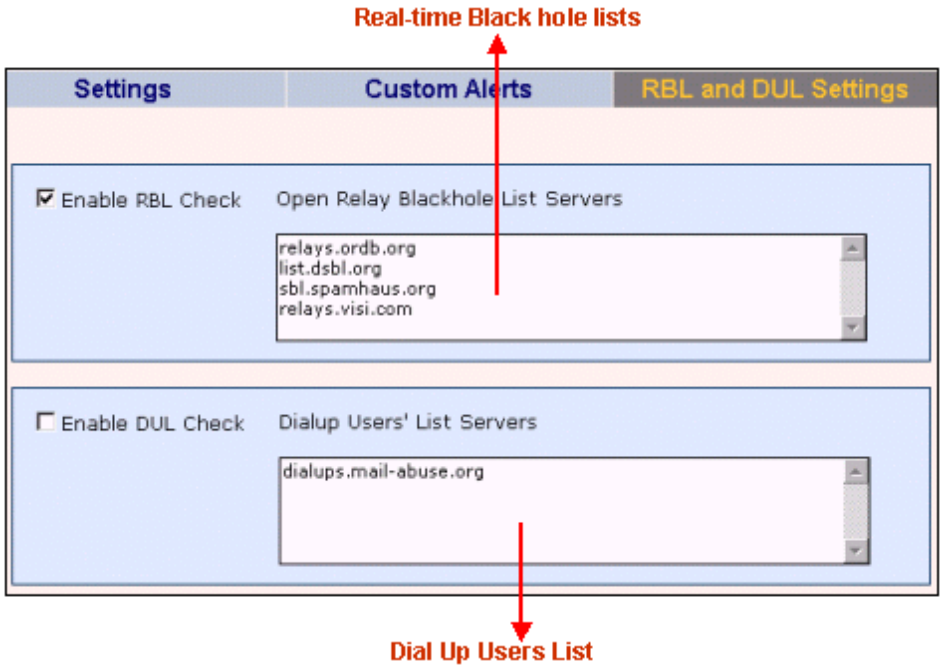

Figure 2 RBL and DUL features

BLOCK SPAMMER WITH BLACK LISTING

Another way to beat a Spam is to refuse entry to e-mail IDs and Domains that are known Spammers. The software should allow you to create a Black List of such users and domains. Software with the following features effectively combats Spam.

- Add e-mail ID of known Spammer to the block list. Any mails received from an ID, included in the list are automatically deleted, without being downloaded into your server.
- Add domains of known Spammers to the black list. Any mails received from such domains are automatically blocked, without being downloaded into your server.

Figure 3 shows a screen from MailScan for Linux, the top selling Anti Virus and Anti Spam software, with features to create Black lists.

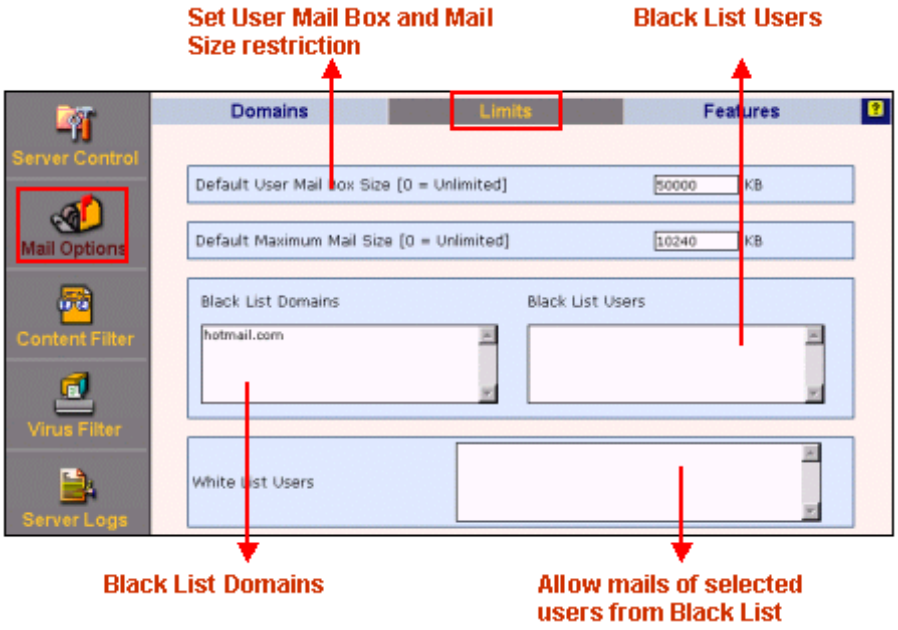

Figure 3 Black List of Users and Domains

DELETE SPAM

The software should allow you to view brief details of Spam and infected mails and delete them. It should also allow you to delete mails that are in the queue as they have not been delivered.

Figure 4 shows a screen from MailScan for Linux, the top selling Anti Virus and Anti Spam software, with features to delete Spam and infected mails.

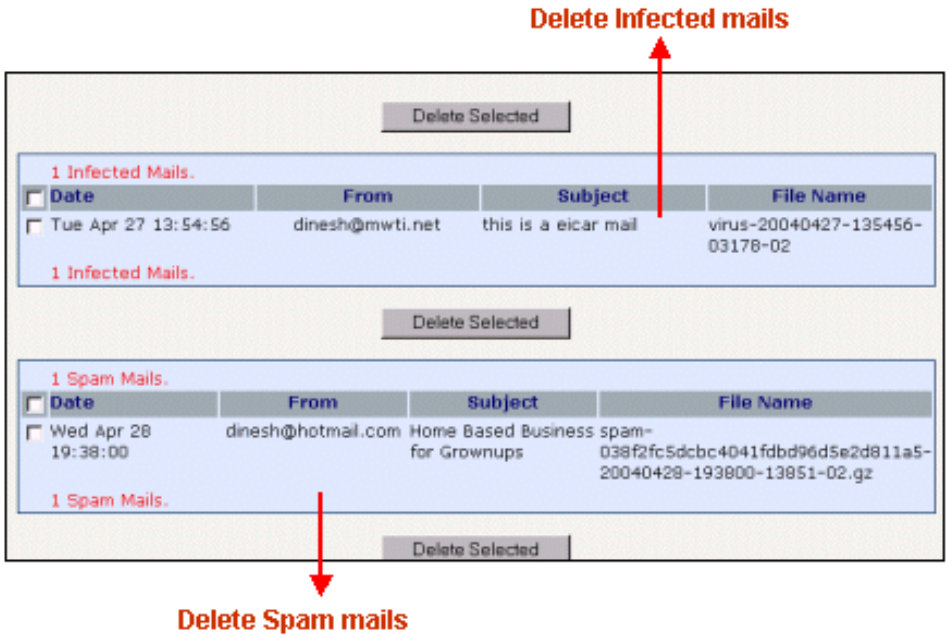

Figure 4 Delete Spam and infected mails

Anti Virus Features

The software should have robust anti virus features as explained next.

VIRUS DEFINITION UPDATES

Every day sees new viruses appearing. Updates are vaccines that detect and remove new viruses. The software must have the means to identify new viruses and remove them. Updates are available as free down loads on our mirror download. The software should allow you to configure MailScan for Linux to connect automatically and download updates from updates download sites.

You should be able to set a daily schedule to automatically download updates at a set time

Figure 5 shows a screen with from MailScan for Linux, the top selling Anti Virus and Anti Spam software, with features to automatically download updates.

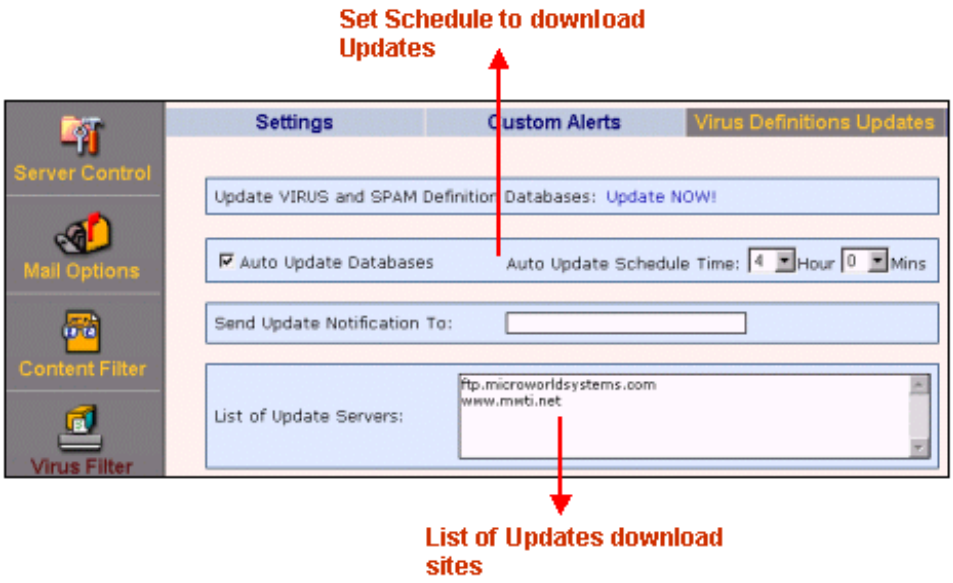

Figure 5 Download Updates

BLOCK SPECIFIC ATTACHMENT TYPES

Some types of attachments are used as virus carrier files. The software should allow you to specify such attachment types and these are automatically blocked. This feature can also be used to stop confidential data being mailed as attachments.

Another feature that is required is a white list of users and domains to whom mails can be sent without scanning. This feature removes double scanning and increases mail delivery speed.

Figure 6 shows a screen with from MailScan for Linux, the top selling Anti Virus and Anti Spam software, with features to automatically download updates.

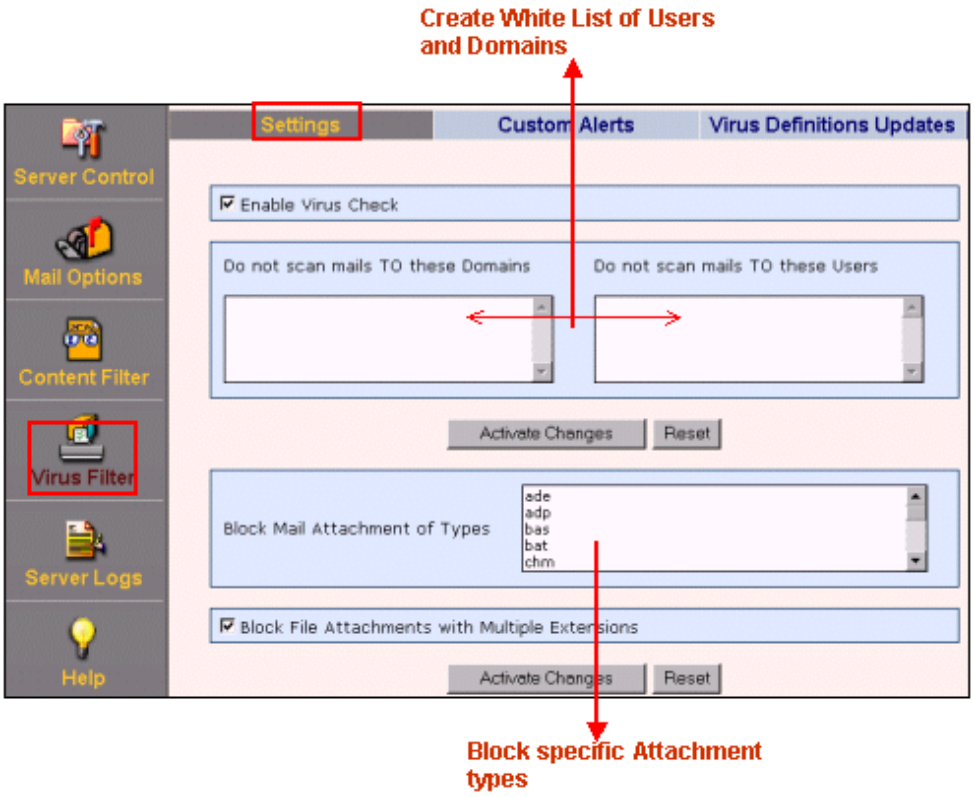

Figure 6 Block Specific Attachment Types

Other Features

In addition the software should have the following features:

- Creating and sending custom alerts when virus or Spam is detected in mails to the mail sender, receiver and admin.
- Move Spam and virus infected mails to a directory or mailbox.
- Start anti virus/Spam and mail service directly from the application without quitting or reboot.
- Allow administrators to import files with details of users, virtual users and access files.
- Archive all mails in a directory or mailbox.
- Provide detailed logs of mail service, Spam and anti virus and an Interface log.

About the Author

Govind Rammurthy is a hard core 'techie' with keen business acumen. He founded MicroWorld Technologies Inc. in 1995 and has been in the forefront in the fight against Viruses and other threats. He leads the team of programmers and QA who have developed world-class product suites, **eScan, MailScan, X-Spam, eTraq, etc.** These products offer the greatest control in the areas of Anti-Virus and Content-Security.

To find out how MicroWorld can help you control Spam, visit http://www.mwti.net/