Remco Hobo

Virus and Worm scanning

January 18, 2005

In this report I will discuss different virus scan programs for Linux and BSD. Virus scanners are widely deployed under Windows, but under Linux and BSD they are not that common. This was because until lately virusses where of no threat to these operating systems. Nowadays virusses can also infect these systems more easily. This is for the most part because these operating systems are becomming more and more popular for desktop applications. More and more people use Linux or BSD as production workstation. The downside to this is that a lot of inexperienced users can cause a lot of damage even by doing simple tasks like reading email or surfing the web. Below I will look at some antivirus programs

1 Vexira Antivirus for Linux (commercial)

A virus defense system designed for easy and dependable virus prevention on Linux based servers. [5]Vexira detects over 74,000 viruses. It is configurable to protect the open file shares and prevent client workstations from saving, reading, writing and executing virus infected files.

After some research this program doesn't seem to be the answer. It is mostly made to be used together with Samba server, a network sharing service for Windows computers. It scans files for Windows virus infected files and has no email scanning functionality.

Key Features:

- Ability to scan files automatically as they are accessed
- Configureable path protection
- E-mail notification
- Blocked access to infected files
- Options to repair, rename, or delete infected files
- Automated Internet updating
- Virus scan archives (.zip, .rar, gz, .tar, etc...)
- Command-line scanner
- Scalable concurrent scanning
- Heuristic detection of new macro viruses
- Low system resource requirements

2 Vexira Antivirus; mail servers (commercial)

For mail scanning, Vexira has Vexira Antivirus for mail servers. It's key features are:

[5]Vexira Antivirus for Mailservers (SendMail, Sendmail+Milter, Qmail, Postfix, Exim, SuSE) is a store-and-forward virus protection application that can intercept TCP/IP port 25 (SMTP) connections or can be started using the Internet superdaemon (inetd). It spools all inbound and outbound e-mail messages and virus scans them using the Vexira Antivirus virus scanner. Messages that are found to be virus free are immediately forwarded to the recipients and infected messages are quarantined and the sender, recipient, and mail administrator are notified.

- Virus detection and quarantine
- Virus scans all in-bound and out-bound email
- Real-Time virus interception
- Can process high volumes of email
- Scalable to the maximum capacity of the server's processing ability
- Configurable warning notifications to sender, recipient or postmaster
- Heuristic virus detection
- Full automatic update of scan engine and virus definition file
- Support virus scanning within archives (ZIP, RAR, LHA, ARJ etc...)
- Detection of malformed messages
- Can be used with other E-Mail messaging servers easily

By intercepting all email traffic on port 25 and, if approved, are forwarded to the real mail server, it can easily be integrated into virtual any mail server. There is no real information on what kind of virusses it scans.

3 Clam Antivirus GPL

[3]Clamav is a widely used open-source virus scanner for Linux, Unix, BSD etc. It is a full solution to the virus threat. It scans both normal files as email data. These files however first have to be accepted to the system as it scans the mbox, Maildir and raw mail files. They aren't deleted the momen they come in as is the case with Vexira Antivirus. Virus definitions are updated automatically and they can be checked for tampering because they are digitally signed.

Key features:

- command-line scanner
- fast, multi-threaded daemon
- milter interface for sendmail

- database updater with support for digital signatures
- virus scanner C library
- on-access scanning (Linux and FreeBSD)
- detection of over 28000 viruses, worms and trojans
- built-in support for RAR (2.0), Zip, Gzip, Bzip2, Tar, MS OLE2, MS Cabinet files, MS CHM (Compressed HTML), MS SZDD
- built-in support for mbox, Maildir and raw mail files
- built-in support for Portable Executable files compressed with UPX, FSG, and Petite

It seems to be a very nice open-source virus scan solution. Looking at the list of sites using this package, it seems to be widely used and used by some big companies.

4 MailScanner GPL

Another open source mail scanner has the original name of [4]MailScanner. This scanner doesn't seem to be of much value. Virus definitions cannot be automatically updated as far as I can find it in the documentation and the key features list seems very odd.

Key features:

- Uses widely-used Postfix, sendmail, Exim or ZMailer packages for reliable e-mail service
- Uses any of 14 different file-based virus scanners, allowing daily updates for the latest viruses Sophos, McAfee, F-Prot, Command, Kaspersky, Inoculate, Inoculan, Nod32, F-Secure, Panda, RAV, Antivir, ClamAV, Vscan Scripts to automate these daily updates are included
- Scans for viruses inside all attachments, including compressed archives
- Checks inside Microsoft Outlook Rich Text format attachments (MS-TNEF files)
- Automatically disinfects any viruses that can be disinfected from the original message attachment (e.g. Word macro viruses)

The list was a lot longer, but most of the key features where of no importance or are expected in all virus scanners. The line below really did it for me:

* Designed to be robust and have extremely long ”uptime”

I cannot imagine any virus program that is not designed for this. I didn't like the documentation so this one I will not use.

5 My choice

The virus scan software had to be open source, that‘s why the first two options are no candidates. Therefore my choice goes to [3]Clam Antivirus. It seems to be robust, it can scan emails and normal files, it has auto-update possibilities. It looks like an all-in-one solution and it is open source. What else you whish for? Due to time constraints I have not installed this virus scanner on my Gentoo machine.

6 Other ways to detect worms/virusses

Besides virus scanners, there are some other ways to fight virusses and worms.

6.1 Snort

One way to detect virusses of worms is to scan traffic. One of these programs is [6]Snort. This program can be used to sniff traffic on predefined interfaces. After configurating the interface to sniff, trusted nets etc. It can sniff for suspicious network traffic. It this happens, it can send email alerts and it sends daily security logs. It even has the capability to update the rules automatically. I have used snort for quite some time and we also use it at the company where I work. A graphical front-end like Demarc further improves it‘s effectiveness.

6.2 Blacklists

A lot of email providers nowadays have their own virus scanners or [2]blacklists. Most of the time you can use these virus scanners and spam filters for free or for little. This way, you can let your ISP handle your email traffic. They might also have a blacklist of providers or addresses that send out spam. This might be a low-cost solution to the whole email problem.

7 CAcert.org

One of the other questions of this excersize was if I found [1]CAcert could play a role as a CA (Certificate Authority) in PKI (Public Key Infrastructure).

First of all, CAcert is an organisation that wants to do what verisign does, be a CA that is trusted by all browsers. This way, a certificate can be issued by CAcert, that then can be used for e.g. secure webpages, secure emails etc. The only difference is that CAcert is free. Users of CAcert can sign each others certificate and thus give the other more points. This way, a web-of-trust is created. With verisign, getting a certificate can be very expensive.

I find what CAcert is trying to do a great idea but i am afraid it will not get off the ground. Nowadays, it cost a great deal of money to get into a browset like IE. Since CAcert isn’t a big company, they don’t have this kind of money. Also, staying in these browsers costs a lot of money. Then there is the fact that companies as verisign will not let this happen without a fight. If CAcert gets into all mainstream browsers, they’ll go out of business. Since organisations as verisign have a lot of money, and CAcert has almost none, they probably will be bullied out of the way. This might be done by bribing significant CAcert members or just by burrying them in bogus court cases.

I really hope that CAcert makes it into all mainstream browsers but I think it can be a while and I have no doubt a lot of mud will be thrown between commercial CA‘s and initiatives like CAcert. To support them, I have registered my SNB domain with them, have added my PGP certificates to their site and have signed my PGP key with the certificate I got after I registered my PGP key at CAcert.

References

[1] http://www.cacert.org, The CAcert homepage

[2] http://www.speed.net/support/faq/spam.html, A spam FAQ; information about blacklists

[3] http://clamav.net, The clamav homepage.

[4] http://www.sng.ecs.soton.ac.uk/mailscanner, the mailscanner homepage.

[5] http://www.centralcommand.com/index.html, The Vexira homepage.

[6] www.snort.org, The snort homepage.