Clam Antivirus: Open-Source Virus protection

Michaël Van Canneyt

March 16, 2014

Abstract

Protecting your precious PC against email and other viruses doesn't have to cost a lot of money: **Clam Antivrus** is an open source virus scanner which can be installed on Unix machines (suitable for integration in mail server's MTAs) but which also has a Windows version for those that are not fortunate enough have a Unix at hand.

Introducing Clam Antivirus

Clam Antivirus is an open-source implementation of a virus scanner which does 1 thing only: it scans a file for known viruses. The virus scanner consists of 2 parts: One is the actual scanner, clamscan: It scans a file to see whether it is infected with a known virus. It reports on the found viruses. The known viruses are kept in a database file. The second part (freshclam) serves to keep this database up-to-date: new viruses are born every day, and existing viruses mutate to more dangerous forms regularly, it is therefore of the utmost importance to keep the database with virus definitions up-to-date. The freshclam program should be run on a regular basis, for instance in a cron job on Unix.

The Unix version features also a client/server model: The scanner runs as a daemon. The clamscan program then sends the file to be scanned to the daemon, for inpection. This reduces startup time and system load, which is quite important on servers than run a heavy-load MTA service.

On Windows, a small GUI frontend exists which allows to perform and schedule scans, and to perform and schedule the virus database update. It does not have 'on-demand' scanning, i.e. scanning files as they are opened by programs. There is, however, a MS-Outlook plugin which can automatically scan attachments in emails. Also a context menu can be installed in the Windows explorer, which allows to scan selected files straight from within the explorer. This should provide ample protection for most purposes.

Note also that on Windows, Clam Antivirus also does not desinfect files. The standard action is just to report an infection, but it can also either remove a file or move it to a safe location ('In quarantine').

All versions can handle compressed files (zip, gzip, bzip2).

Installation

The Unix version (currently 0.70) can be downloaded in source form or as installable packages (for various linuxes), from sourceforge:

```
http://clamav.sourceforge.net/
```

The Windows version (currently 0.33)can also be found on sourceforge:

Figure 1: Windows ClamWin program finished a scan

`http://winclam.sourceforge.net/`

Installation on Windows is straightforward: there is a Windows installer, which is like any other installer. It is best to tell the installer to download the latest virus database after it was installed.

On Unixes, the installation can be performed with a binary installer if one is available, but it can be done just as easily by compiling it. Compilation and installation is quite straightforward and described in detail in the (detailed) documentation (in PDF format).

Scanning for viruses

Scanning for viruses is straightforward: On Unix, run the clamscan command with the names of the files or directories that should be scanned as arguments. Combined with cron and the 'find' command, a system-wide scan can easily be implemented and scheduled, in a fashion that is tailored to the system on which it is installed.

Since Unix systems are not very vulnerable to viruses, the main use is actually scanning of email for Windows clients. This requires integration of clamscan in an MTA, as discussed below.

On Windows, 3 things can be done to scan for viruses:

1. Select some files in the Windows Explorer, call up the context menu and select 'Scan for viruses with ClamWin'.
2. Start clamwin (a tray icon is available on the taskbar), which will display a nice window where directories are shown; The selected directory will be scanned (figure 1 on page 2).
3. Schedule a scan. This can be done in the preferences dialog of the clamwin program.

All three methods will result in a scan report.

Email protection

On Windows, a plugin for MS-Outlook is installed which allows to scan emails and their attachments for viruses. The author does not use Outlook, so was unable to test this.

On Unix, the virus scanner must be integrated in the MTA program, such as Sendmail, Postfix or Qmail. This is done through external programs such as 'milter' for Sendmail (delivered with clamav), or 'qmail-scanner' for Qmail (must be downloaded separately). The documentation contains a complete (and long) list with programs that can be used, together with download locations.

Conclusion

While it does not completely secure a PC, Clam Antivirus will stop most viruses: Those that enter through email. It will not stop viruses (worms) that enter through open TCP/IP ports or use other system vulnerabilities, but given that most viruses today enter a system through email, it is definitely worth installing it: It doesn't cost money, although donations will be appreciated, and may result in even better protection in future.