www.sxc.hu

KlamAV brings Clam Anti-Virus to your KDE desktop

KLAMMING UP

Linux may not be as virus-ready as Windows, but who wants to harbor pointless malware? Now you can hunt for viruses with KDE's KlamAV, a desktop front-end for the ClamAV Open Source virus protection system.

BY ROBERT HOGAN

If you receive email and download files from untrusted sources, your computer can end up as a repository for malware. Although very few of these harmful payloads can actually damage a Linux system, these malevolent programs are still unnecessary, and, in some cases, you may run the risk of passing them on to Windows colleagues. It makes sense, therefore, to implement some form of virus protection.

One of the great success stories of Open Source software is ClamAV, a signature-based virus filter for mail gateways originated by Tomasz Kojm and now supported by a growing community and a world-class update infrastructure. The goal of KlamAV is to bring the superb ClamAV virus detection system to the KDE desktop.

Getting Clam and Klam

KlamAV is starting to appear with some of the popular Linux distributions. If

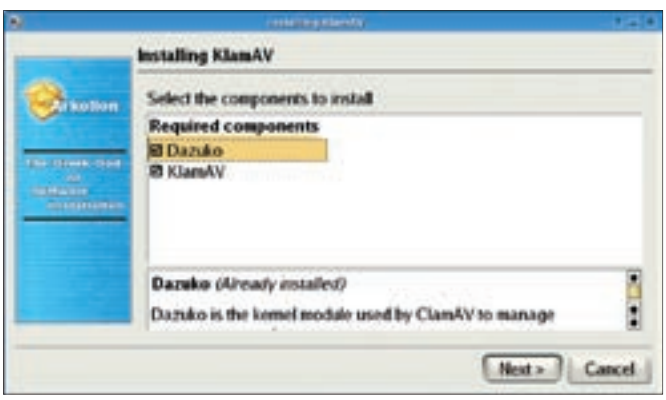

Figure 1: Arkollon, a graphical installer for Linux, installing KlamAV.

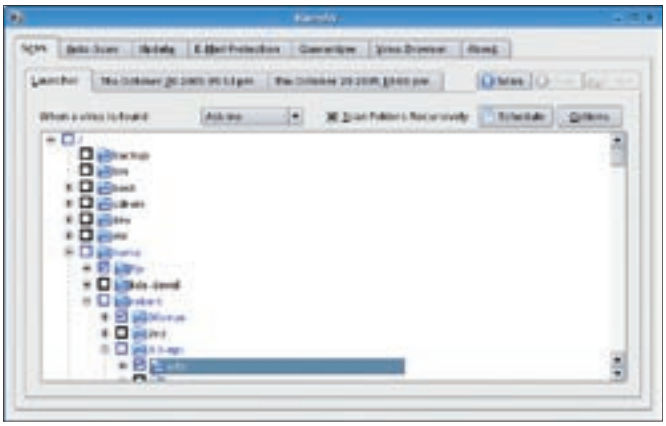

Figure 2: Selecting directories for scanning. Note that there are scans in progress on the hidden tabs.

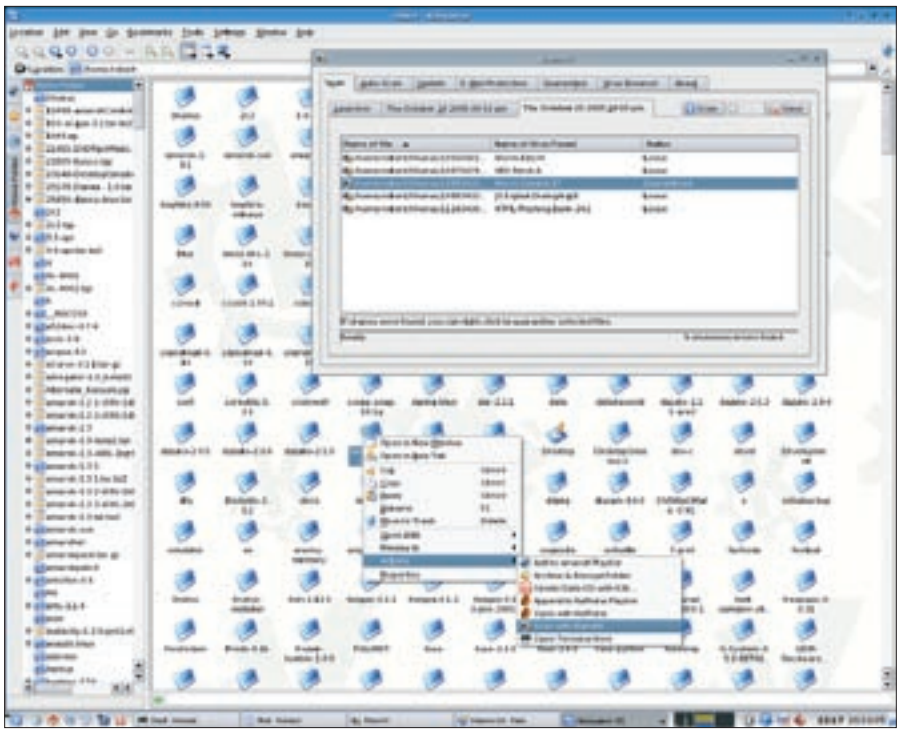

Figure 3: While scans are running, you can select other files or folders for scanning from Konqueror.

KlamAV isn't available with your system, you can install it in a number of ways. Your first option is the installer available at [1]. Double-clicking on the downloaded file will extract and run Arkollon[2], which will manage the compilation and installation of KlamAV. Manual installation is also an option if you download the source package. ClamAV is a prerequisite for first-time installations, so be sure to get it first at [3].

Scanning Files and Folders

The *Scan* tab in the KlamAV main window lets you select the files and folders you wish to scan. All the folders on your system are available through the *Scan* tab. You can select any combination of folders and scan them in a single step. KlamAV can run multiple scans simultaneously.

Right-click on a file or folder in Konqueror to initiate a scan through the Konqueror context menu. KlamAV will open a new scanning tab and continue any current scans uninterrupted. You can also set the time for any future scans.

A popular feature in many commercial anti-virus products is on-access scanning – the ability to scan files whenever they're accessed by the system. Thanks to Dazuko [4] and integrated support for Dazuko in ClamAV, on-access scanning is also available to the KlamAV user. Dazuko is a kernel module that intercepts system calls to files and allows external programs, such as ClamAV, to decide whether access should be granted. It is packaged with KlamAV for the sake of convenience, although, because not all kernels are created equal, you may have to deselect it at installation time and take the trouble to install it manually. Configuration is straightforward and you can decide under what conditions the files will be scanned (e.g., when they're executed, opened, closed, read, or written to). If you want to use this feature, find the combination that suits you, but be aware that this is perhaps the most experimental element of ClamAV/KlamAV, and that the whole area of on-access scanning in Linux is not yet fully mature.

Scanning Email

An irritating shortcoming on the current Linux desktop is that most efforts to scan incoming mail completely freeze your email client while the messages are being downloaded. Thanks to the elegance of the ClamAV architecture, KlamAV offers a component called klammail to address this problem. klammail is essentially a command-line utility that accepts email on standard input, scans it with a ClamAV process running in the background, and pumps it back out on standard output. Because the scanning process is daemonized, there are no expensive start-up times associated with using klammail.

If the mail is infected, klammail will encapsulate the virus in a warning mail and display a warning dialog. To use this handy utility, simply select the *E-Mail Protection* tab in KlamAV and ask it to configure your mail client to scan incoming mail. If your mail client is not supported for automatic configuration, the KlamAV mail-scanning design supports any email client that allows you to 'pipe' mail through an external program and provides instructions to guide you through the simple setup process.

Updates

The most important part of managing anti-virus protection on your home desktop is staying up to date. ClamAV possesses an update network that rivals and often exceeds commercial vendors in the speed and accuracy of its response to new virus outbreaks. A recent study by Electric Mail found that, when compared with two of the world's top five commercial anti-virus solutions, ClamAV was first to respond 77% of the time for the last 50 new virus variants checked! [5]

KlamAV allows you to turn on permanent access to the superb ClamAV update service with just a couple of clicks.

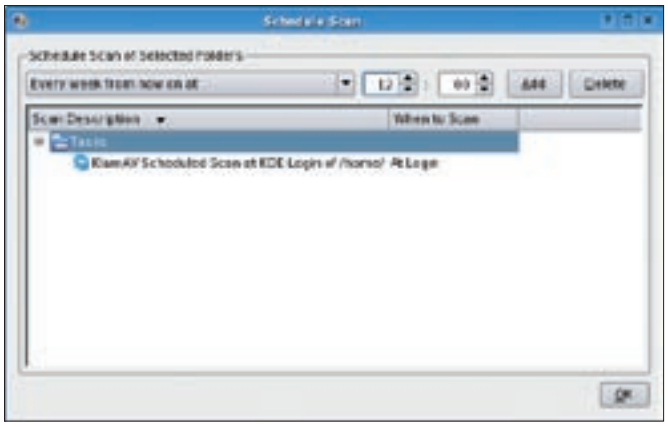

Figure 4: Setting up scheduled scans.

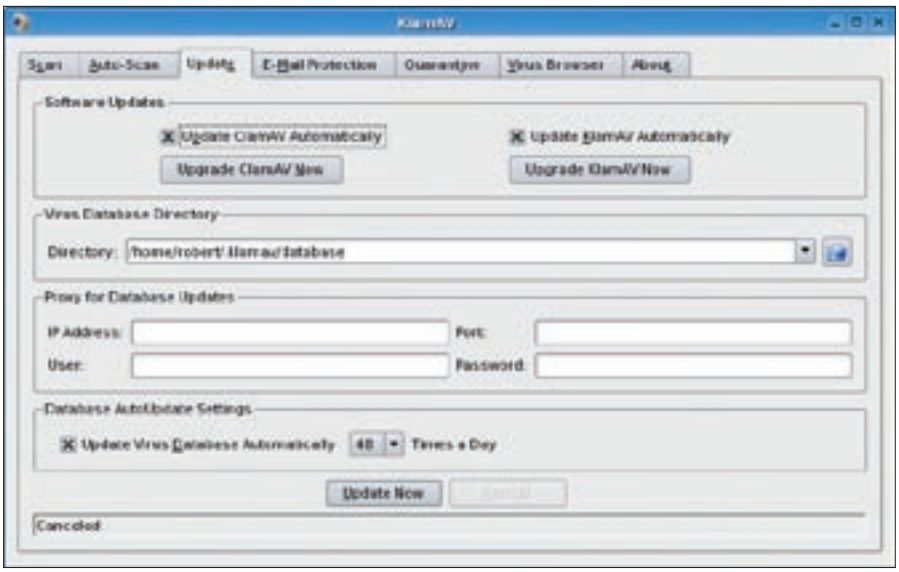

Figure 5: KlamAV looks after the updates so you don't have to.

To check for updates every half hour, simply select the *Updates* tab, select *48 times a day*, and click on *Update Virus Database Automatically*. Now click *Update* and forget everything you've just read because you won't need to do it again.

Apart from updates to your signature database, it is also important to keep your copy of ClamAV up to date. The ClamAV engine contains important detection checks that are continually improved and updated. When you select *Update ClamAV automatically* in the *Updates* tab, KlamAV will check for a new version of ClamAV every time it starts up. If a new version is found, it will download the new version for you and even compile and install it. Even if you forget to select this option, KlamAV will still warn you if your copy of ClamAV is out of date and offer to download and install the new version.

Virus Found! Don't Panic!

Finding viruses is all very well, but the more challenging task is deciding what to do with suspicious files. Virus names are less than informative, and everyone at some point has found themselves negotiating Google for enlightenment on names like *Gen.1024-PrScr.1*. KlamAV attempts to integrate this next step in the discovery process as seamlessly as possible.

When KlamAV finds a virus, the virus is displayed in the main scanning interface. You have the option to quarantine all of the files immediately (at which point you can investigate them farther under the *Quarantine* tab) or use the right-mouse button to select one or more files for selective research and quarantine.

Figure 6: Inspect the signature database with KlamAV's virus browser.

If ClamAV has discovered a version of Worm.Mytob, you can select *Search Worm.Mytob with VirusPool*. This option will open the *Virus Browser* tab. ClamAV's signature database will appear, and an embedded browser window will display information about Mytob from VirusPool, a nearly comprehensive online database of known viruses.

While you're in the virus browser, you can take the opportunity to research any of ClamAV's known viruses using a number of online resources. The ability to research viruses is also available from the quarantine manager, again by right-clicking on the culprit.

Finally

KlamAV is the humble KDE cousin of the formidable ClamAV virus protection system. The KlamAV virus scanner brings the power of ClamAV to your KDE desktop and provides an easy-to-use user interface for scanning files and managing viruses.

The future of malware management on the Linux desktop lies in a number of directions, among them rootkit detection, heuristic analysis, the continued growth of on-access scanning, and memory-residence detection. These areas will become more important as Linux adoption grows, and ClamAV certainly provides a sound foundation towards meeting the evolving needs of the home Linux user.

If you would like to see KlamAV in action, go to the homepage and check out the video tutorial, or dip straight in and download the installer at [1]. ■

INFO

[1] KlamAV Home Page: *http://klamav.sf.net*

[2] Arkollon (originally part of Apollon): *http://apollon.sf.net*

[3] ClamAV Home Page: *http://www.clamav.net*

[4] Dazuko is available at *http://www.dazuko.org*

[5] *http://www.linuxpipeline.com/166400446*