Virus protection tools for the Linux environment

VIRUS CHECKERS

So you want a virus checker? We'll show you what we found when we toured some of the top scanners for the Linux environment.

BY JAMES MOHR

Since the famous Bliss virus in early 1997, the media has been relatively quiet on the topic of Linux viruses. However, depending on your source, there are anywhere from a few dozen to over 400 viruses, Trojans, and other kinds of malware that infect Unix and Linux. Compared to the tens of thousands of viruses, worms, and other infections that afflict Windows, this number is certainly small, and the chances are much lower that you will be directly affected (or infected) by a Linux virus. But as you learned in the preceding article, virus checking in Linux is still important.

Getting a Scanner

If you are using Linux as a file or email server in your company, you definitely need to consider installing an appropriate virus scanner. In my case, the dozen or so viruses I get each week, is a motivator to take an active approach in fighting viruses.

When starting this project, I expected to find only a handful of companies which provide Linux anti-virus products. While I did find some that appeared to be simply jumping on the Linux bandwagon, I also found several that take a very active and professional approach to viruses on Linux.

In this article, I'll investigate some of the most popular virus checkers for the Linux environment.

The Roundup

For the article, I chose only products I could *download* and check for free, even if the download version is just an evaluation copy. I didn't cover products that are only available on a CD you have to order. The CD-only products seemed to be an exception, because I was able to round up a wide range of products. In some cases, more advanced products like email or file server versions were not available for download.

In addition to checking the products for recognizing and removing the viruses in our test lab, I also evaluated the scanners for ease of use. I expect the installation and use of commercial software to be easy. You shouldn't have to be an experienced system administrator to install it. My original intent was to talk about "workstation" versions, but not every company provides a version labled "workstation," and in those cases, I chose a product that appeared similar in functionality.

BitDefender

The Linux version I downloaded was called BitDefender-Console-Antivirus-7.0.1-3, which comes as an RPM file. Although BitDefender [1] does not support the same range of operating systems as other vendors, it does provide a fair bit of variation in its products. For example, there are versions for sendmail and sendmail milters, Qmail, PostFix, and Courier. In addition to the Linux scanner, they also provide a free version of their scanner for Windows.

Although starting the first scan was more straightforward than starting some of the other products, the only file Bitdefender initially identified as a virus was the EICAR test file. Added to this, the online help didn't match the manpage. I used a command right out of the manpage that was supposed to include "archives," but none of the .zip files were scanned.

It was not until I used the *--all* option that it scanned files other than standard *Windows* executable files (i.e., files ending with .exe, .com, .bat). Interestingly enough, even without the *--all* option, it *did* scan the files *letter32.txt* and *body2.doc*.

Listing 1: BitDefender Sample Output

```
Results:
Folders           :1
Files             :64
Packed            :0
Infected files     :32
Suspect files      :0
Warnings          :0
Identified viruses:7
I/O errors         :2
```

Listing 2: ClamAV Sample Output

```
---------- SCAN SUMMARY ----------
Known viruses: 40507
Engine version: 0.86.2
Scanned directories: 1
Scanned files: 69
Infected files: 69
Data scanned: 4.91 MB
Time: 3.705 sec (0 m 3 s)
```

Still, even when I used *--all*, things did not work out well. The product reported *every* .zip file as being "OK," despite the fact other products identified them as containing viruses.

When I changed the file names to *.exe* or *.doc*, the files were scanned and identified as archives, *and* the zipped files inside were identified as the same virus found by other products.

I discovered that in the configuration file, there was a list of "extensions" that the program uses to decide whether it should scan a file or not. When I added "zip" to the list, the files were scanned and identified correctly. It seemed as if, without being in the list of "known extensions," the file would not be scanned by default. Considering that Linux does not work with file extensions the same way that Windows does, and this is a Linux virus scanner, it seemed that the tool was still scanning files as if it were on a Windows machine.

In comparison to other products, the primary configuration file contains only a few settings, although most settings are self-explanatory. However, the documentation does not explain how to add default start options to this file (if it is even possible.)

In all honesty, I have to say that BitDefender did respond *very* quickly to my email query about these issues. Something that not every vendor did. In their response, they admitted that the documentation needed to be clearer and were very helpful getting issues resolved.

Although I did have problems getting the product to run smoothly, once I got things figured out, it did identify all of the viruses correctly. As that is the key issue, I think one should still consider looking at BitDefender, especially because the Linux version is free for home users.

Clam AV

ClamAV [2]was the only Open Source anti-virus product I found. I initially thought it would either be necessary to recompile ClamAV, or else I would only be available to install it for a handful of distributions. To my surprise, packages are available for all of the major Linux distributions, as well as for many other OSes, like Solaris, AIX, FreeBSD, and even BeOS. There is also a ClamAV version specifically for sendmail milters, as well as for different Windows versions, such as a "native" version and another version that is part of the official Cygwin repository.

I downloaded and installed the RPM of clamav-0.86.2 and, in contrast to other products, the manpages were all installed as they should be; also, *man -k clam* showed all of the appropriate manpages. Getting my first scan was very simple. ClamAV recognized all of the viruses, something not every commercial product did.

You can't really talk about a workstation or server version of ClamAV as you get all of the software in a single package. In addition to the traditional command-line scanner, also included is *clamd*, a multi-threaded daemon that enables on-access scanning for Linux and FreeBSD. The clamd daemon requires you to compile and install the Dazuko kernel module.

Although ClamAV does not have the greatest number of command-line options, it definitely holds it's own with commercial products in terms of configurability. Unfortunately, there didn't appear to be a configuration file to specify default behavior. Thus, you need to specify the options each time you run the program. Still, it is easy enough to write a shell script – I would definitely not overlook ClamAV just because of this. *clamd* and the updater program have configuration files, each with a wide range of options.

The command-line scanner provides a couple of nice features. For instance, you can scan files sent to *clamscan*'s standard input (i.e., *cat filename | clamscan -*). Although other products ended with different exit codes, depending on whether they found a virus or whether an error occurred, ClamAV provided details of what these exit codes are, a feature that seems to be unique among all of the products I examined. Both of these features allow ClamAV to be easily integrated into other applications, such each email servers.

F-Prot

F-Prot [3] from FRISK Software International is perhaps the most well-known anti-virus software product for Linux. At one time, the F-Prot virus scanner was the only Linux anti-virus product that was available for free to home users. Although it is no longer unique in this regard, the F-Prot scanner is still available as a free, no-time-limit version for home users. Versions are also available for Windows, a few UNIX versions, and IBM eServers.

I downloaded and installed the free workstation version of F-Prot, which is known as version 4.6.0. The product came as an RPM file. There were no extra files containing a PDF, README or anything similar. Instead, I had to look through the files contained within the RPM packages in order to learn what documentation was available, and also to determine what program I actually had to start.

It seemed that I had to guess about the behavior of certain options, as F-Prot has very limited documentation in comparison to other vendors. Although the documentation is sufficient to get the product into operation, it does not go much beyond that. Also, the f-prot manpage refers to a man-page for the main configuration file (*f-prot.conf*), which wasn't included, although the file itself was. Still, the number of options available is comparable to commercial products, and it some cases, f-prot is easier to use.

Looking through the configuration file, I found a number of options that seemed only to apply to a system daemon or other program running on a file or email server, implying that the free version is a scaled-down version of another product.

Every virus was accurately identified by F-Prot. Since recognizing viruses is the whole point, F-Prot is definitely worth a look.

F-Secure Anti-Virus

F-Secure [4] has perhaps the widest assortment of anti-virus products. For example, their F-Secure Anti-Virus Enter-

Listing 3: F-prot Sample Output

```
Results of virus scanning:

Files: 71
MBRs: 0
Boot sectors: 0
Objects scanned: 129
Infected: 67
Suspicious: 1
Disinfected: 0
Deleted: 0
Renamed: 0

Time: 0:01
```

Listing 4: Sophos Sample Output

```
67 files swept in 2 seconds.
2 errors were encountered.
60 viruses were discovered.
60 files out of 67 were infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com, email support@sophos.com
or telephone +44 1235 559933
End of Sweep.
```

prise Suite contains products ranging from Windows Workstations to Citrix Servers, Linux Gateways, Samba Servers, and more.

I downloaded the 30-day workstation version 4.52. This version came as a .tgz file containing a shell script with embedded binary. In the instructions, F-Secure says that the task of removing the product is done “simply by removing the installation directory.” However, the removal leaves a number of other files lying around the system. They suggest using *find* to look for files, which is something I would not expect from a commercial product.

One nice thing was that during the installation, you are prompted for several options to define how the program behaves. However, unlike other products, the number of questions is kept to a minimum.

It was disappointing to discover that this version could *not* properly scan a number of viruses inside of zip files. Instead, it reported an “internal error.” This happened on the same files that the free versions and all of the other commercial products correctly reported. For a commercial product, not recognizing all of the viruses was unsettling and I found nothing on the F-Secure web site to help to get me around this problem.

In addition to the command-line scanner, there is also a daemon, which one starts through an rc-script or by the command-line scanner. This version also provides a shell script, which inserts a cronjob to do a scan or update your database. Although I expect any good admin to be able to insert a crontab entry, I still found this feature useful, as it guides you through all the necessary steps.

The configuration file provides a fair number of different configurations, including which directories to scan or not to scan, what syslog facility to use (if that’s how you choose to log your scans), actions to take, file extensions to scan, and so forth. In contrast to other products, by default, *fsav* also scans files *without* extensions.

AntiVir

AntiVir was developed by H + BEDV Datentechnik GmbH [5]. The AntiVir scanner is provided by default with many versions of SuSE Linux, as well as for free for home users from their web site. I tried for several days to download the free, non-commercial version and repeatedly got server errors, so I ended up downloading the “Professional” version 2.1.4.8, which is available for a 30-day trial.

My initial negative impression was compounded by the fact that even on the page for their “business solutions, ” it seemed that the text was translated by someone whose native language is not English. In some cases, I couldn’t understand what they were trying to say. These problems extend to the online documentation and even the installation script.

An “evaluation license” of AntiVir was provided with my version of Linux, and since I had already installed the product, I figured the best thing I could do was to remove the previous version first. Although *rpm seemed* to have removed all of the files, the RPM database still thought the package was installed, so apparently something went wrong. So it was unclear how to remove it completely and the response from H + BEDV support was not very helpful.

Because I had not actually purchased the professional product, it ran in “DEMO mode.” This meant it was not able to update the virus definitions. Fortunately, all of the viruses I had were old enough that that were already included, but if you are planning to test it in the future, this could be a problem. Although the installation text, README, and so forth were all in English, the product provides only a German version of the “UNIX Server” user’s handbook as a PDF file.

When I was finally able to download the personal edition version, I could not find out how to remove the professional version. It had not installed an RPM, and the only thing I found in the documentation or on their web site indicated that an “update” was done by simply re-running the install script, so that’s what I did. It identified the fact that a version was already installed and tried to update it. Since the personal edition comes with a key, I no longer got the message it was a demo version. Whether or not this was the correct procedure is still unclear even with email from H + BEDV support.

In comparison to other software, the installation took a fairly long time because it asks you *a lot* of questions about how the software should be configured. For the professional version, I understand and even appreciate things like this. However some of the questions were things a normal user would not fully understand, so for the “personal” version they were more an annoyance than anything else.

Part of the product is AvGuard, which provides “on-access, real-time scanning of files” and requires you to compile the Dazuko kernel module, which was originally developed by H + BEDV.

Kaspersky Anti-Virus

The Linux Workstation version is available as a 30-day download, and I downloaded version 5.5-2. Of the products I looked at, Kaspersky [6] definitely gave the impression of being the most professional product. Although I do not want to give the impression that others were unprofessional, Kaspersky was perhaps the most comprehensive package I looked at in terms of both features and presentation.

In addition to the workstation version, Kaspersky has file server versions for various Linux and UNIX platforms; an email server version supports sendmail and Qmail. You’ll also find a sendmail milter version and a Samba server version. Depending on which product you select, there are a number of different pre-defined license packages.

Included with the download was a 68-page PDF, which definitely went above and beyond the documentation provided with other products. The .tgz-file I downloaded contained rpm, deb, and tar.gz files, so I installed the RPM. During the installation processes I was asked if the accompanying Webmin module should be installed. If Webmin is not installed, you can always install it later.

The workstation version also provides a system daemon, which it starts from an rc-script. This intercepts filesystem operations before the applications can access it. In general, this function is very useful, but different applications "froze" while the daemon was running as they tried to access virus-infected files. I also noticed when monitoring my system that there were some very significant performance spikes in system usage when running *kavmonitor*. In some cases, the CPU load was at or as close as you can get to 100%, however, even these occasional performance spikes were not necessarily a show stopper for me.

The configuration file was very extensive, with all of the options one expects, plus you can tell it to execute a particular program depending on whether it has identified a virus or simply suspects one. For example, you can send a notification (by email) to root, write a syslog entry, and so forth.

I did run into some problems running a scan as a non-root user. Based on some options in the default configuration file, I was not able to write to a couple of the files. However, you can tell the scanner to read from a different configuration file and in doing so, have it write to places where your account has the necessary permissions.

The command line options were daunting, simply because there are a lot of options, but the doc provides a good example that got me started. Needless to say, it accurately identified all of the viruses I had.

The update mechanism is as extensive as the program itself and allows you to do automatic updates of the virus database, even through a password protected proxy server.

Sophos

This product was provided by Sophos PLC [7]. Finding the appropriate version on their web site was not all that easy, as I ended up guessing that "Other" meant Linux. In this case, "Other" also meant most other non-Windows operating systems, such as the major UNIX vendors and even SCO. I even found a version for OpenVMS.

It was not immediately clear which product version I downloaded, as the file I downloaded was named *linux.intel.libc6.glibc.2.2.tar.Z*. After I installed the products, I found the version of the primary scan tool to be 3.97.0.

The installation was fairly simple, but unlike other tools, Sophos requires you to first manually create a special user and group. You then run the the enclosed shell script, which appears to simply copy the files to their appropriate location, not an RPM package. Removal of the product is accomplished manually by following a list of files and directories that you need to delete.

Getting the first manual scan was not as easy as with some products, as it wasn't entirely clear what actually needed to be started. Since there was no RPM file, I could not scan the contents for any man-pages. Still it only took a few minutes to figure out.

Although I installed the product as root, I ran into a number of problems when I tried to run my first scan, as it reported a missing directory. After creating the directory, there was yet another directory missing. Going through this process a couple more times, I finally got it running. Why these directories were missing was not explained by anything on the Sophos web site. I did get a fairly quick response from Sophos when I emailed asking why these directories were missing, and they were helpful getting my issues resolved.

Doing the initial scan was really easy, and the tool quickly scanned through my viruses. However, it "skipped" scanning 5 of the files and did not identify the virus in 5 other files. When using the *-all* option, it appears *not* to scan certain archive types by default. So, to have it scan *all* of my infected files, I had to use both *-all* and *-archive*.

I tried to figure out which file types it did not scan by default. I used several options to get it to list the clean files, either alone or as part of the complete output, but to no avail. Although I eventually got it to scan and detect all of the infected files, it did take a lot of work.

Vexira

This product is provided by Central Command, Inc. and I downloaded version 1.2.0 of their Vexira Command Line Virus Scanner [8].

Vexira is not really "installed" in the traditional sense. You simply unpack the archive and have all the files you need right in front of you. Although this might be fine for a free personal system, I was disappointed with it for a professional product.

In comparison with other products, there are not as many different variations of the Vexira Antivirus. In addition to the version that I downloaded, there are versions for mail servers (even sendmail Milters), Samba servers, and a product simply for "Linux servers."

Initially I felt the command line somewhat cumbersome. When starting the command, it was not immediately obvious what options and in what order you need to simply display a list of infected files. By default, the tool stops at every infected file and asks what you want to do.

My personal expectation is that when you scan the system you simply want to know if there are viruses before you do anything. I felt being prompted for every single file as the default was a bit annoying. Because computers are now really commodity goods, you expect things to "just work" easily enough so you don't have to read through all of the documen-

Listing 5: Vexira Sample Output

```
Summary of scanned objects' types
--------------------------------
 files (total)       |      68
   in archives       |      59
 mail parts          |       6

Summary of malware pieces found
--------------------------------
 iworm               |     67
 virus               |      3
 mutant              |      1

Summary of actions taken on alert
--------------------------------
 skipped             |     71

Error summary
--------------------------------
 inaccessible target |        2
```

tation just to get it to do a basic scan.

Unlike other products, Vexira does not have an automatic update of the virus database. Instead, you need to use FTP to download and install the database manually, then replace the existing database file. According to the vendor, this FTP download step is necessary for "security reasons" in case your DNS server is "breached." However, this would also apply to their FTP server, so I personally do not see any real advantage to requiring a manual download of the database. Although a typical Linux administrator should be able to bang out a quick script that does everything automatically, there are enough mechanisms available today for the program to figure out whether the file you download is legitimate or not.

Since the primary goal of installing a virus scanner is to find then remove viruses and other malware, one shouldn't get bogged down in details like these, however. Vexira found all of the viruses the other products found, which is the basic point of a virus scanner. One thing I really liked about Vexira was the output of the scan. When it found a virus Vexira would report (for example) “killable” or “NOT killable.” Plus the tool listed the number of the different types of malware it found, such as Internet worms, viruses, and even mutants. This feature is something that seemed to be fairly unique.

Despite the nits I picked with the the Vexira anti-virus scanner, I had a very good feeling about the product, both from a technical standpoint and regarding my interactions with the company in general. I received replies to my email queries faster than I did with most of the other companies, and they were open to suggestions as well as criticisms.

No Single Solution

The bottom line is that I couldn’t find one specific product that did *everything* “right.” As is often the case with software, you need to make a decision about which features are most important to you. The products that immediately recognize all of the viruses may still have characteristics you don’t like, and, depending on your needs, one product may have a feature that makes it stand above the others. ■

INFO

[1] Bitdefender: *http://www.bitdefender.com*

[2] Clam AV: *http://www.clamav.net*

[3] F-Prot: *http://www.f-prot.com*

[4] F-Secure: *http://www.f-secure.com*

[5] H+BEDV: *http://www.hbedv.com*

[6] Kaspersky: *http://www.kaspersky.com*

[7] Sophos: *http://www.sophos.com*

[8] Vexira: *http://www.centralcommand.com*

THE AUTHOR

James Mohr is responsible for the monitoring of several datacenters for a business solutions provider in Coburg, Germany. In addition to running the Linux Tutorial web site *http://www.linux-tutorial.info,* James is the author of several books and dozens of articles on a wide range of topics.