

# KNOPPPIX HACKS™

Includes  
Knoppix on  
CD-ROM

*100 Industrial-Strength  
Tips & Tools*



O'REILLY®

*Kyle Rankin*

HACK  
#78

## Scan for Viruses

Ridding a network of Windows computers of a virus or worm can seem impossible. Viruses may cause computers to reboot and infect new machines while you are in the process of removing them. Through the use of the live-software installer, Knoppix provides a solution to this catch-22.

Viruses and worms are a common problem in the computing world today. It seems every other day a new virus or worm comes out, and anti-virus vendors must quickly update their signatures to block the new outbreak. Unfortunately not everyone has a virus scanner installed on his system, or if he does, it might not be kept up to date. When the worst happens, you must make sure that the virus doesn't spread to other computers on the network or damage your files. If you install a virus scanner, you must be sure that the virus can't find a way to infect, disable, or hide from it.

There are several advantages to using Knoppix as a virus scanner over the alternatives:

***You are booting off of read-only media.*** While the home directory in Knoppix is writable from a ramdisk, all the system files are on read-only media. Even if a virus can somehow infect Knoppix, it isn't able to modify any of the system files, and any files it can infect are deleted at the next reboot. Also, all the underlying partitions are mounted read-only by default. Unless you purposely mount a partition read/write, it is not possible for an infection to spread to your partitions.

***The possibly infected system is not running.*** Knoppix is running outside of your underlying system, so any viruses that might have been loaded into memory have been erased, and the hard drive itself is, in effect, frozen in time, so you don't have to worry about a virus evading deletion. This also means you don't have to worry about the virus spreading, so you can connect the machine to the network while it is running Knoppix to read any advisories or download any files you might need.

***You are booting off of a completely different operating system.*** While viruses have been written for Linux in the past and more will be written in the future, it is still rather uncommon. Let's face it; you are probably scanning a Windows system for a virus or worm that runs only on Windows, and Knoppix runs off of a completely different operating system, so even if you accidentally click on a virus-infected file, it doesn't launch the virus. If the virus has infected other machines on the network and is scanning systems to infect, you don't have to worry about reinfection while you are running off of Knoppix.

***It's free.*** While it is still advisable to have virus protection running on a Windows system at all times, virus protection can be expensive—not

only due to the initial cost, but also to the annual subscription fees to get virus-definition updates. If you can't afford virus-protection software, you can at least scan your system periodically with Knoppix for free.

F-Prot is a free virus scanner that you can run under Linux. You can install F-Prot with Knoppix's live-software installer, covered in "Use the Knoppix Live Installer" [Hack #27]. The live installer needs a working Internet connection to download the program, and the program itself needs to be able to download updates as well.

Click K Menu → KNOPPIX → Utilities → Install software, select f-prot, and click OK to start the installation. Once the installation finishes, click K Menu → KNOPPIX → Extra Software → f-prot to start the F-Prot GUI.

After you launch F-Prot, immediately select option 4, "Do Online Update," to make sure that you have the latest list of virus definitions (see Figure 7-2). Once the update is finished, choose "Select partition(s)" from the F-Prot GUI, or if you have already mounted the partition, you can choose "Select a directory/file" to pick the directory to scan. Once you choose a directory, you are dropped back to the main menu where you can then choose Scan to start the scanning process. A progress meter appears, and the length of the virus scan varies, depending on the size of the directory you are scanning.

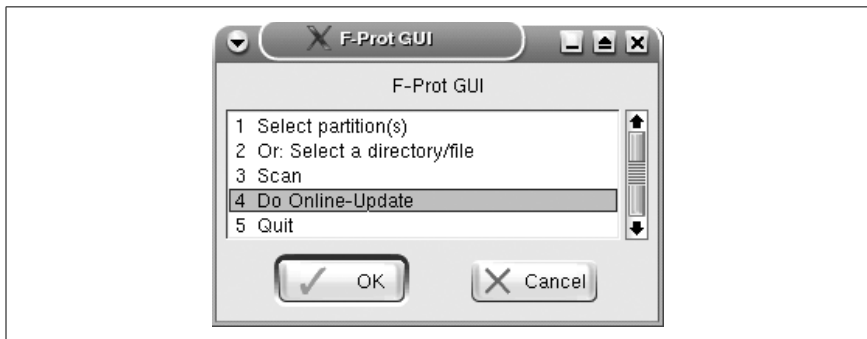


Figure 7-2. The F-Prot GUI

Once the process is finished, F-Prot displays a report that lists the different files it has scanned. The information you are probably most interested in, whether you are infected or not, is listed at the very bottom of the file. There, you should see how many files F-Prot has scanned, and under that, you should see whether F-Prot has found any viruses. If you are clean, you should see "No viruses or suspicious files/boot sectors were found."



If you do have an infection, it can be time-consuming to filter through the output to find which files are infected. To make this easier, run *grep* to search for the word Infection on the F-Prot output file that is in your home directory by typing the following command in a terminal: **grep Infection ~/report-2004-05-17-0.txt**.

Once you have a list of suspicious or infected files, you can mount the partition read/write and delete or rename the files. If you are a Windows expert who is comfortable with registry edits, you can follow the steps in “[Edit the Windows Registry](#)” [Hack #76] to remove any registry keys the virus might have left behind. You might also want to view advisories on the viruses that F-Prot finds on <http://www.cert.org> or other security sites, and see if perhaps there is a patch you can download to protect your system from this virus or worm in the future. Now is a good time to save any patches you might need to your hard drive, so you can boot back to your computer without having to connect to the network, and install the patch as covered in “[Download Windows Patches Securely](#)” [Hack #79].