
Hardening the Linux desktop

A selection of easy-to-use tools for keeping your systems secure

Skill Level: Introductory

[Jeffrey Orloff \(jeff.orloff@gmail.com\)](mailto:jeff.orloff@gmail.com)

Director of IT/Security
SafeWave, LLC

25 Nov 2008

Although GNU/Linux® has the reputation of being a much more secure operating system than Microsoft® Windows®, you still need to secure the Linux desktop. This tutorial takes you through the steps of installing antivirus software, creating a backup-restore plan, and making practical use of a firewall. When you finish, you'll have the knowledge and tools you need to harden your Linux desktop against most attacks and prevent illegitimate access to your computer.

Section 1. Before you start

To get the most out of this tutorial, follow the steps provided for each task with either a computer running GNU/Linux or a virtual machine with GNU/Linux as the operating system.

About this tutorial

This tutorial introduces you to the basics of GNU/Linux security and shows you how to protect, or *harden*, your desktop against attacks. It gives you step-by-step examples of how to:

- Protect your computer against malware attacks

- Configure a firewall to keep attackers out
- Back up important files and recover files after a successful backup
- Install updates to your operating system and other software
- Password-protect the bootloader

These same fundamental security concepts for making your desktop safe can also serve as a foundation for hardening your Linux servers.

Objectives

After completing this tutorial, you will be able to harden your GNU/Linux desktop and prevent attacks against your computer and its data. You will be able to install and configure software to help protect your desktop against malware that can give an attacker access to your computer. You will also be able to use a firewall to protect against inbound and outbound traffic, back up and restore your data, and apply other tricks that further harden your system.

Prerequisites

This tutorial is written for beginning GNU/Linux users. It assumes that you have a basic understanding of the GNU/Linux operating system and have experience downloading and installing software.

System requirements

To use the examples in this tutorial, you need the GNU/Linux operating system installed on a computer or as a virtual environment with root access. You also need an active Internet connection with the ability to download software.

The examples use Ubuntu, so it is recommended that you use a Debian fork of GNU/Linux. Although the examples will work on a virtual machine running GNU/Linux, you should not use a Live CD.

Section 2. Myths about GNU/Linux security

For years, GNU/Linux users have enjoyed the notion that their operating system is

superior to Microsoft Windows in terms of security. Unfortunately, what attackers stand to gain from compromising a computer or network has also changed over time.

Originally, most attacks against computers stemmed from hackers seeking notoriety in their community. There were cases of malicious hackers seeking to obtain sensitive information for monetary reasons. But the concept of stealing financial or confidential information for profit wasn't the primary goal of hackers—until recently.

Today, well-organized criminal organizations employ malicious hackers for the sole purpose of breaching computer security systems for financial gain. Over the years, monetary losses due to computer breaches has been estimated in the hundreds of billions.

When mischief was the primary driving force for malicious hackers, Windows systems were their primary target. Windows was easy for anyone, not just computer enthusiasts, to use. And so desktop computers began to appear in just about every home, school, and business around the world; and they were being used by people with below-average computing skills. With such a large pool of novice users, malicious hackers had no shortage of easy targets.

Windows also became a favorite target of certain malicious hackers because of its proprietary software. Some attacks were motivated by the desire to make a socio-political statement and bring negative publicity to Microsoft, which was not seen as a supporter of the open source community. These attacks also began to foster myths about security in computing circles.

Is GNU/Linux more secure than Microsoft Windows?

One of the most popular myths surrounding computer security is that GNU/Linux is more secure than Windows. Many factors come into play when you determine how secure a system is. The most important factor is how the system was configured. It is highly unlikely that a GNU/Linux system configured by a complete novice would be more secure than a Windows systems configured by a highly skilled specialist.

This tutorial addresses the proper configuration of the GNU/Linux desktop. By taking the steps to configure your computer system properly, you can make sure your system is secure. Blindly accepting the "Linux is more secure" myth can lead to trouble.

Is GNU/Linux virus-free?

Another computer security myth is that viruses don't attack GNU/Linux computers. Although fewer viruses have been written to attack GNU/Linux systems than

Windows systems, GNU/Linux viruses do exist. Threats to GNU/Linux systems are also posed by other forms of malware, such as Trojan horses, rootkits, and spyware. These threats are addressed in the [next section of this tutorial](#).

The number of attacks against GNU/Linux systems has been steadily increasing. One reason is simply that the number of users switching to GNU/Linux operating systems is increasing. As these operating systems have adopted the graphical user interface (GUI) concept, GNU/Linux has become an easy-to-use, less expensive replacement for Windows.

Another reason for the increase in attacks against GNU/Linux systems is the fact that more attacks are financially motivated. Attackers no longer care what type of operating system their target is running—they just want the high-priced data that is housed in the computer. If the targeted computer runs Windows, they use Windows exploits. For computers running GNU/Linux, they attack an entirely different set of vulnerabilities.

As you progress through this tutorial, you'll see some of the basic steps you can take to help prevent unauthorized access to your GNU/Linux desktop computer. New vulnerabilities are always being discovered. You need to make it a priority to stay informed and take appropriate action to maintain the security of your computer.

Section 3. Protecting against malware

Malware is short for *malicious software*. Any program or file whose purpose is to damage or disrupt a computer system or network is malware. To understand what you need to protect as a GNU/Linux user, and how to go about protecting your computer, you first need to understand how malware can attack GNU/Linux and what design fundamentals in the operating system help prevent against malware infections.

In order for malware to spread between systems, and in order for it to cause damage, the program or file needs to be executed. GNU/Linux was designed so that users should not be running under the root (administrator) account; therefore, programs and files do not have the ability to execute without explicit permission. Without the ability to execute programs in this login state, malware can't install itself, or propagate, through a GNU/Linux system due to user permissions. The user permissions security feature is built into GNU/Linux and is one of the most effective tools against the spread of malware.

Malware written for Windows won't run on a GNU/Linux computer. Just as Microsoft Office can't be run directly from a GNU/Linux system, the malicious programs and

files don't run because the binary executables are written for Windows. If you try to launch a malicious program written for Windows in a GNU/Linux environment, the program won't know what to do because its instructions are written to read, write, and execute according to the Windows architecture. This also helps prevent malware from being written for GNU/Linux, because changes in the various distributions of the operating system are enough to render some malware useless.

Although some aspects of malware are irrelevant to the GNU/Linux desktop, there are still several reasons why you should be concerned about it. Actively scanning for malware helps prevent it from spreading. Even if you do not execute a malicious program on GNU/Linux, you might still pass the program on to another computer. For example, if you're using multiple environments, it would be easy to pass an infected file from your GNU/Linux system to a Windows system through e-mail, via a USB drive, or over a Samba share.

Another example stems from cross-platform malware that is coded to respond differently depending on the host operating system. If the malware detects Windows, it attacks as such. If Red Hat is detected, different commands are run.

You also need to consider the increasing popularity of platform-independent environments such as OpenOffice.org, Perl, and Firefox. Malware can be engineered to attack specific vulnerabilities that are platform independent. For example, the MSIL.Yakizake worm sent an e-mail to each person in the host's Thunderbird address book. The messages were custom tailored to the DNS suffix so that the language of the mail was correct.

Finally, you must keep an eye out for malware packages written specifically for GNU/Linux. Rootkits have long been the Achilles heel of GNU/Linux administrators. They are part of the same software family as Trojan horses. A *rootkit* is a collection of tools that lets an attacker gain access to the root (administrator) account on your computer. These malware packages go by different names, such as tOrn and ARK, but the end result is the same: your computer or network is no longer under your control.

Install anti-virus protection: ClamAV

To fight the growing malware problem, in this section you install ClamAV, rkhunter, and chrootkit on your box and then learn how to configure and scan your system for some of the nasty files that could compromise your security. When installing ClamAV, you have two options for how you want to run the program. The first method allows you to scan files and folders manually. The second method connects ClamAV to a daemon so that it's always running. For a desktop, the latter method is the ideal method of installation.

Start by powering up and logging into your computer. Then, follow these steps:

1. Select **Applications > Accessories > Terminal** from the menu bar.
2. Once the terminal is launched, enter the following command: `sudo apt-get install clamav-daemon`
3. Press **Enter**. You're asked for your password. Enter the correct password, and then press **Enter** again. Doing so installs a package called `clamav-freshclam`; this is the updater package for the application.
4. You're informed how much disk space will be used when you install the software. Type `y` at the prompt, and press **Enter**.

The installation process begins; it should take only a couple of minutes. When the installation process ends, you're alerted to the fact that your virus database is older than x days and that you should update it as soon as possible.

Aside from installing anti-virus software on your computer, keeping the virus definitions up to date is the most important step in keeping your files free from malware. Virus definitions are the patterns of code that are unique to different malware programs. When an anti-virus scanner matches this code against the definition in the database, it alerts you that there is an infected file on your computer.

Malware writers release new infectious files into the wild daily, so it's important to constantly update your virus-definitions database. If the definition for a particular piece of malware isn't in this database, the anti-virus scanner won't know it's malicious code and will let it run and do whatever damage it was programmed to do.

Update your virus definitions

Because you installed `freshclam` with ClamAV, you can update your virus definitions immediately from the terminal. Follow these steps:

1. At the prompt, type the following: `sudo freshclam`
2. Press **Enter**. Again, you're prompted for your password; enter it, and press **Enter**. Running this command updates your definitions to the most recent database. Understand that this doesn't mean your virus definitions are updated automatically -- you must run `freshclam` in order to get the latest definitions.
3. To see if there are new definitions, type the following at the prompt: `sudo freshclam -v` The information returned lets you know if your definitions are up to date or out of date.

Now that you've updated your virus definitions, you're ready to start ClamAV. At the terminal prompt, type `clamscan` and press the **Enter** key. This command runs a manual scan of your home folder and provides a report of how many directories and files were scanned. You're also told how many infected files were found.

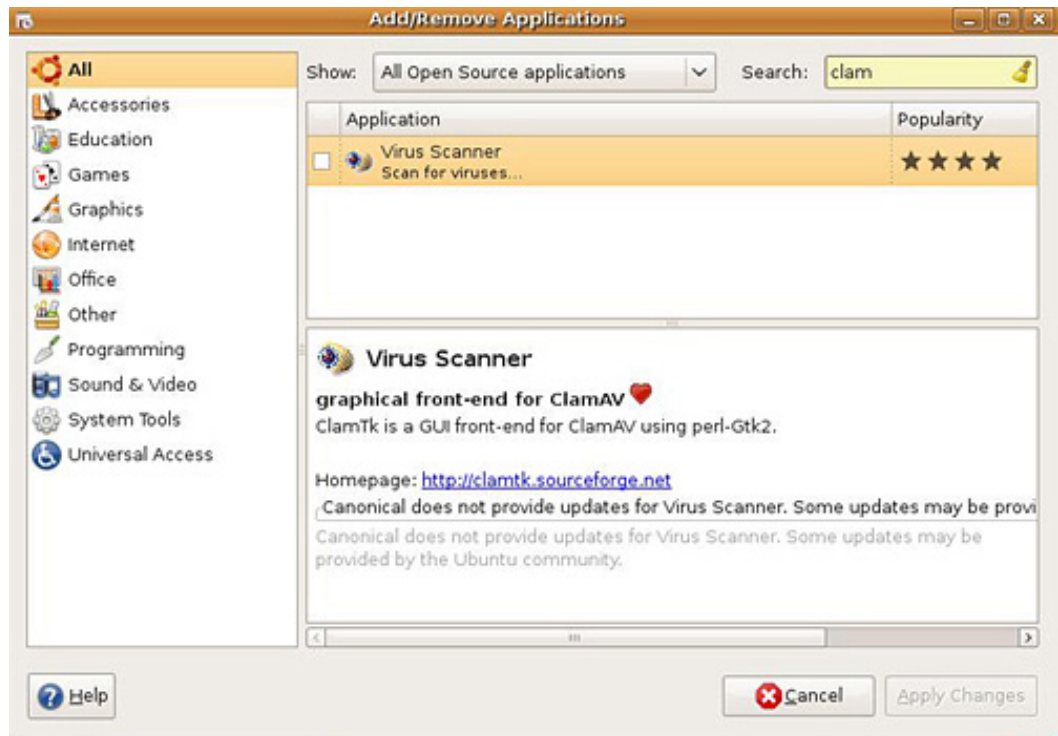
Because you installed the daemon version of ClamAV, you also have the option of typing `clamdscan` at the terminal prompt. Press **Enter**, and a user named ClamAV is created. If you want ClamAV to scan system files, you can add this user to the group that owns the files you wish to scan.

Install a GUI for ClamAV

Because this tutorial is aimed at beginners, this section explains how to configure ClamAV using a GUI called ClamTK. To install it, follow these steps:

1. Close the terminal, and choose **Applications > Add/Remove**.
2. In the resulting Add/Remove Applications window, you need to change the applications that appear. At the top of the screen, choose **All Open Source applications** from the **Show** drop-down menu.
3. Type the word `clam` in the search box, and press **Enter**.
4. When Add/Remove Applications finds ClamTK, it's listed as Virus Scanner in the main section of the window (see Figure 1). Select the check box next to **Virus Scanner**. You may be prompted to enable the installation of community-maintained software. If you're asked about this, click the **Enable** button.

Figure 1. Installing ClamTk using the Add/Remove tool



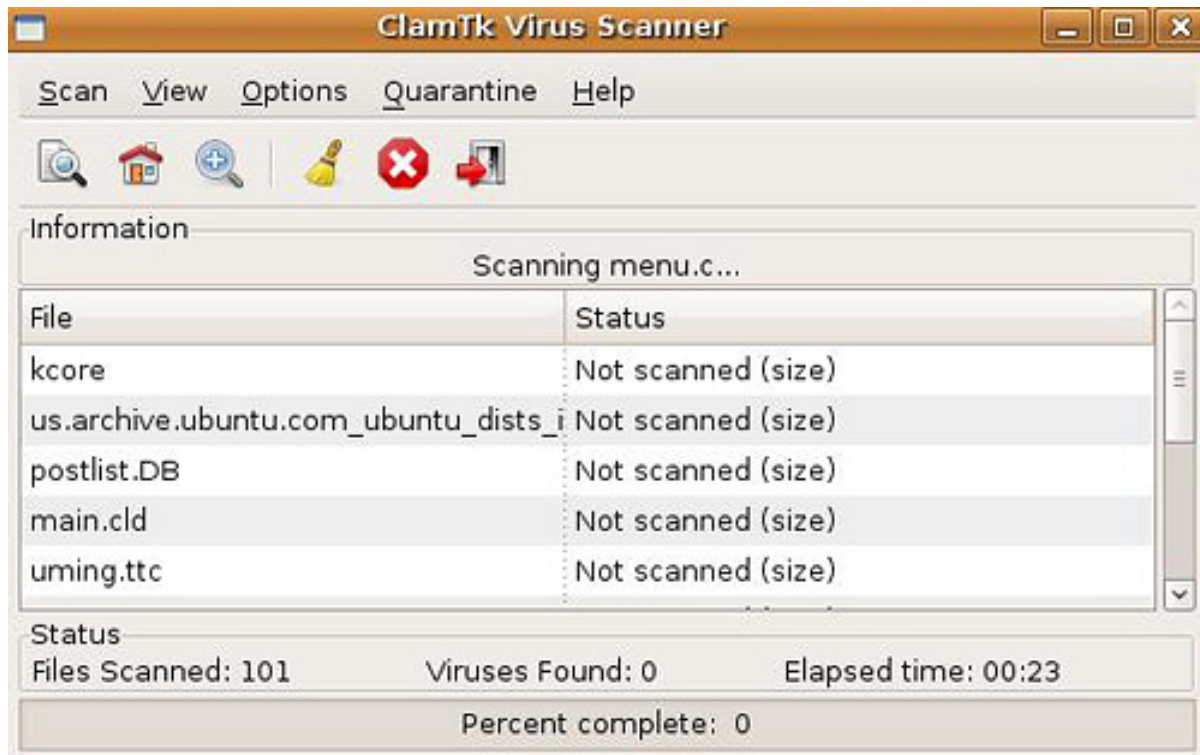
5. Click **Apply Changes** at bottom right, and then click **Apply**. You're asked for your password; enter it, and click **OK**.
6. Once the installation is complete, you're presented with a pop-up window informing you of this. Click **Close** to continue.

You can launch ClamTK from the desktop by choosing **Applications > System Tools > Virus Scanner**. But if you try to scan certain files, or try to update the signatures (virus definitions), you may be told that you need to be logged in as root in order to do this. Because you don't log in as root, you have to take a different approach to opening ClamTK so that you can use the program.

To open ClamTK, press **Alt-F2**, type `gksu clamtk`, and click **Run**. Doing so launches the ClamACV GUI with the rights needed to get the program working. From this window, you can navigate through the commands using the menu. This lets you select the file or directory you wish to scan by choosing from a tree rather than typing a path in the terminal.

Like most commercial scanners, ClamTK lists the file on one side of the window and then the status of the file next to it. Figure 2 shows files waiting to be scanned. If one of the files listed was infected, it would be noted here. At the bottom of the window, you are shown how many files have been scanned and how many infected files were found.

Figure 2. Scanning for malware using the ClamTk GUI



If you find that malware has infected any files, be sure that the file isn't an essential system file before you delete it. This is especially true if you're using a dual-boot computer, because you can scan Microsoft Windows directories using GNU/Linux and ClamAV.

Protect against rootkits

Probably the most dangerous malware that GNU/Linux users face is the rootkit. To fight against the possibility of attack via rootkits and other exploits, in this section you install rkhunter and chkrootkit to scan your desktop for suspicious files that may have been installed by an attacker to gain control of your computer.

Install rkhunter

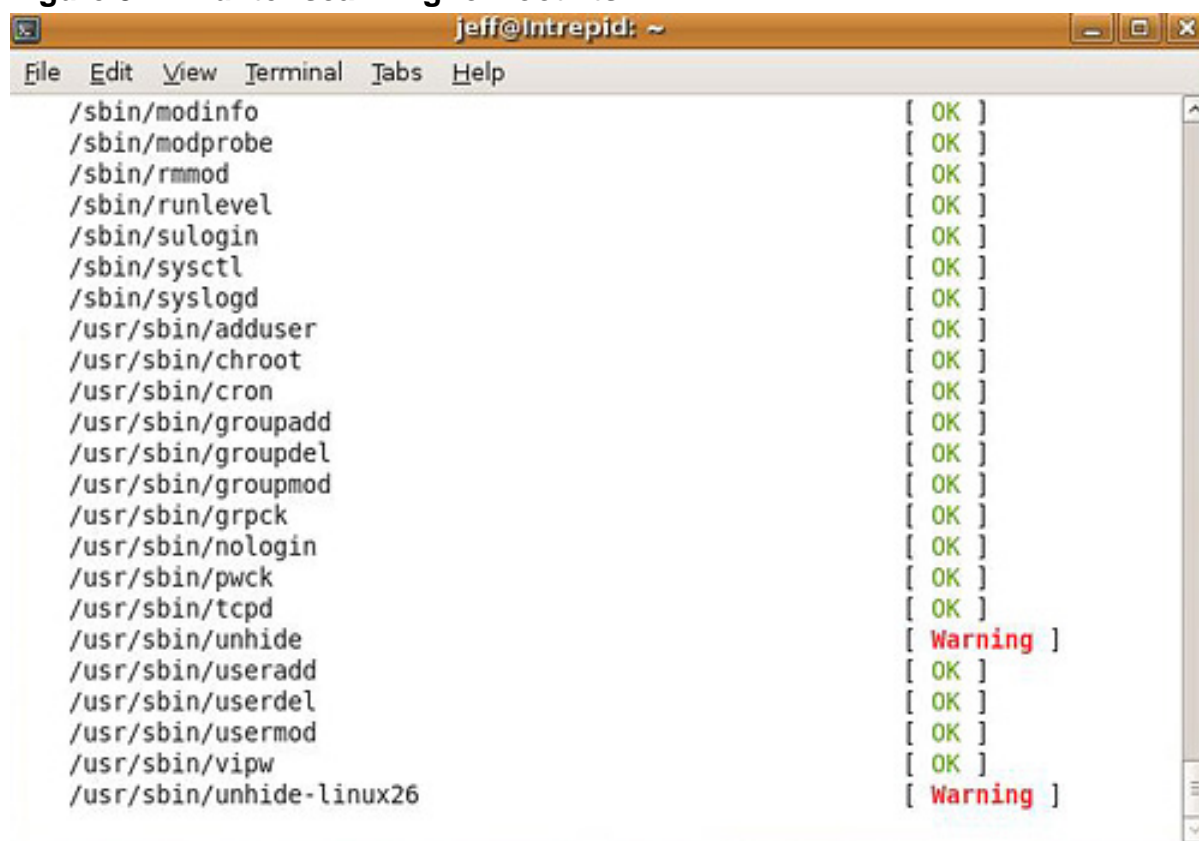
To install rkhunter, follow these steps:

1. To navigate back into the terminal, select **Applications > Accessories > Terminal**.
2. In the terminal shell, type the following command to install rkhunter: `sudo aptitude install rkhunter`
3. Press **Enter**, and the installer begins to run. You're informed about how

much space will be used by this software. Type `Y` at the prompt, and then press **Enter** to begin installing the software.

Once rkhunter is successfully installed, you can run it to check your desktop for a number of exploits. Type `sudo rkhunter --check` at the terminal prompt and press **Enter** to begin the scanning process. When it's running properly, you should see a list of directories with the word *OK* or *Warning* next to them. After these directories are checked, you're asked to press **Enter** to continue the scanning process. Rkhunter next runs a scan for known exploits that could be installed on the desktop. This too appears as a list in your terminal as it runs, as shown in Figure 3. Once this is complete, you're asked to press **Enter** again. This time, rkhunter scans the ports on the computer that are commonly used for backdoor access.

Figure 3. Rkhunter scanning for rootkits



```
jeff@Intrepid: ~  
File Edit View Terminal Tabs Help  
/sbin/modinfo [ OK ]  
/sbin/modprobe [ OK ]  
/sbin/rmmod [ OK ]  
/sbin/runlevel [ OK ]  
/sbin/sulogin [ OK ]  
/sbin/sysctl [ OK ]  
/sbin/syslogd [ OK ]  
/usr/sbin/adduser [ OK ]  
/usr/sbin/chroot [ OK ]  
/usr/sbin/cron [ OK ]  
/usr/sbin/groupadd [ OK ]  
/usr/sbin/groupdel [ OK ]  
/usr/sbin/groupmod [ OK ]  
/usr/sbin/grpck [ OK ]  
/usr/sbin/nologin [ OK ]  
/usr/sbin/pwck [ OK ]  
/usr/sbin/tcpd [ OK ]  
/usr/sbin/unhide [ Warning ]  
/usr/sbin/useradd [ OK ]  
/usr/sbin/userdel [ OK ]  
/usr/sbin/usermod [ OK ]  
/usr/sbin/vipw [ OK ]  
/usr/sbin/unhide-linux26 [ Warning ]
```

After scanning the ports, press **Enter** to scan startup files, groups and accounts, system configuration files, and the filesystem. Then, press **Enter** again to check the applications on your computer. Once this scan is complete, rkhunter provides you with a report and creates a log file for you to review later.

Like ClamAV, rkhunter needs to be updated so it can find the latest vulnerabilities and exploits. From the terminal, type `sudo rkhunter --update`, press **Enter**, and then enter your password. This command updates the version of rkhunter

installed on your system.

Although most anti-virus software won't run properly alongside another company's anti-virus program, rootkit hunters will run symbiotically with one another. For more comprehensive protection, you can install chkrootkit and run it alongside rkhunter.

Install chkrootkit

Follow these steps:

1. While still in the terminal, enter the following command at the prompt:
`sudo aptitude install chkrootkit`
2. Press **Enter** to begin the installation process.
3. Once chkrootkit is installed, you run it just like you do rkhunter. At the prompt, type `sudo chkrootkit` and then press **Enter**. Immediately, chkrootkit begins scanning for known vulnerabilities and exploits. Once it completes its scan, you're brought back to the terminal prompt.

If rkhunter or chkrootkit finds anything out of the ordinary, you're informed, but that's all. These programs don't delete files from your computer. If you're alerted to something by either program, research the exploit or vulnerability that has been reported. First, make sure that what was found isn't a false positive. Then, determine the necessary steps to eliminate the threat of your desktop being compromised. Sometimes, you only need to update the operating system or other software. Other times, you have to locate a rogue program and eradicate it from your system.

Section 4. Using a firewall

Once you've scanned your system for any malware that could provide an attacker access to your computer, you should take the next preventative step and use the firewall built into your operating system. Ubuntu, by default, runs iptables as the firewall on every distribution. Upon installation, this firewall allows all incoming and outgoing traffic by default. To use the firewall, you need to create rules to lock down your desktop.

You can configure iptables via the terminal, but this tutorial uses a GUI called Firestarter to write rules for you. Firestarter isn't installed on Ubuntu by default; to install it, open the terminal and type this command:

```
sudo apt-get install firestarter
```

Press **Enter**, and provide your password to begin the installation process. When Firestarter has been installed, close the terminal window and select **System > Administration > Firestarter** to launch the program.

Configure Firestarter

When you launch Firestarter, you're taken through a setup wizard. Follow these steps:

1. The first screen introduces this process. To continue, click **Forward**.
2. The next screen asks you to provide information about your network device. If you're using an Ethernet cable to connect your computer to a router, the Ethernet device should be set to eth0, as shown in Figure 4. If you have DHCP running on your network, be sure this option is selected before you click **Forward**.

Figure 4. Configuring the network device in Firestarter



3. If you're sharing your Internet connection with other computers, the next screen lets you configure this (see Figure 5). Once you've configured your network setup, click **Forward**.

Figure 5. Configuring Internet connection sharing



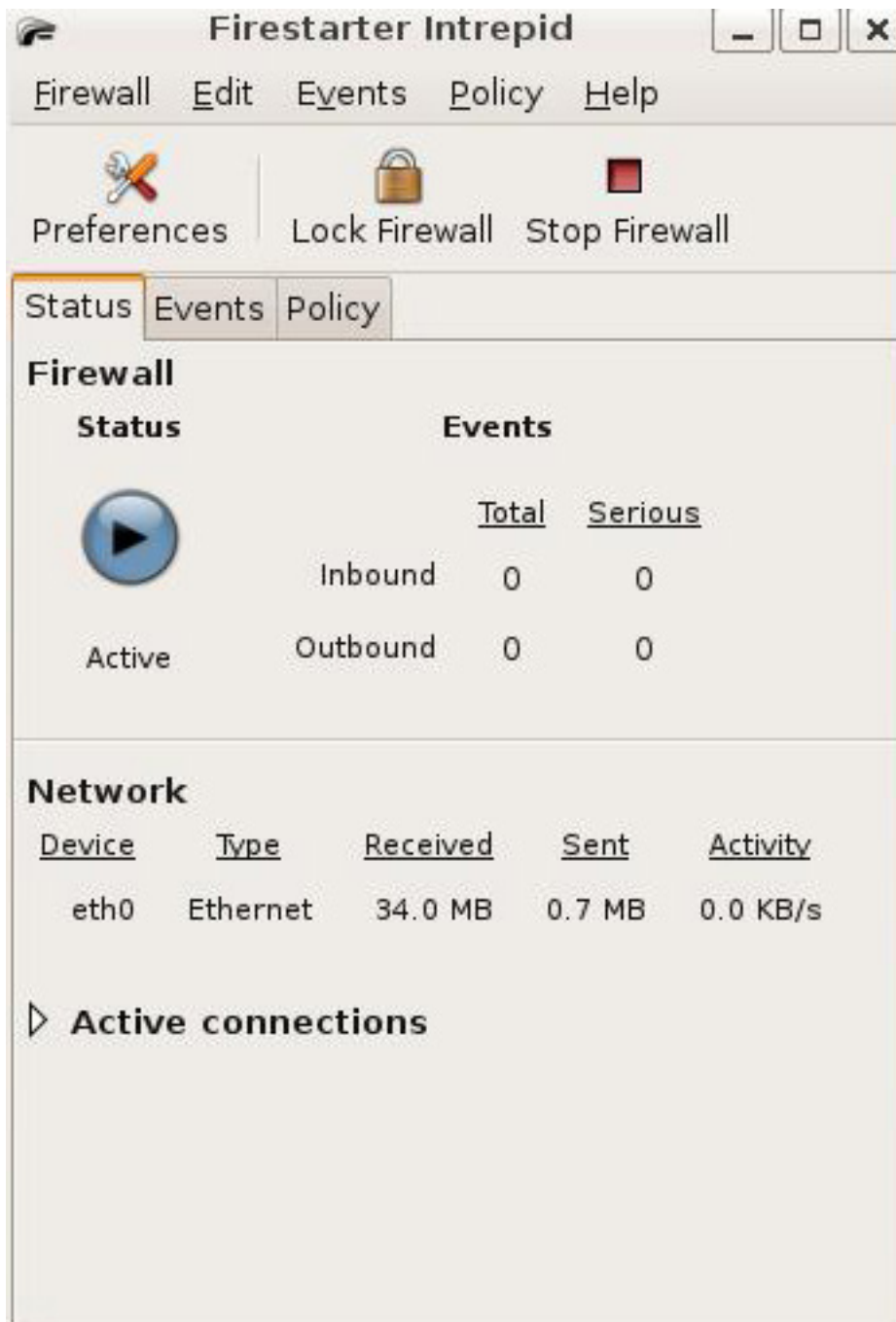
4. You've completed the setup wizard. Click **Save** to start the firewall.

Before you begin configuring Firestarter policies, you should include it in your startup programs so that it can protect the computer each time you boot up:

1. Select **System > Preferences > Sessions**.
2. Click **Add** to bring up a window where you can type the startup command. Enter `Firestarter` in the **Name** box, and type the following in the Command box: `sudo /usr/sbin/firestarter`
3. Click **Add**, and then close the **Sessions Preferences** window.

Figure 6 shows Firestarter actively monitoring a computer. But in order to use it to stop illicit traffic, you need to first create policies.

Figure 6. Firestarter



Create policies in Firestarter

Firewall policies are the rules that determine how a firewall handles incoming and outgoing traffic. Policies can be set to prevent traffic to or from a specific IP address, a specific site, or even a port on a computer. When creating policies, it's important to remember that although blocking certain traffic may make your network/computer safer, it can also hinder the ability of people to work. You need to find a balance

between security and functionality.

Make sure Firestarter is open on your desktop. Firestarter blocks any inbound network traffic that isn't a response to a connection established by a secure host. If you didn't initiate the connection, Firestarter blocks it by default. To create a new policy that allows an inbound connection, follow these steps:

1. Click the **Policy** tab in Firestarter, and make sure the **Editing** option is set to **Inbound traffic policy**.
2. Click **Add Rule** at the top of the window. When you do this, a new window appears, asking what incoming connections to allow (see Figure 7).

Figure 7. Adding an inbound traffic policy



3. In the text box, type the network, hostname, or IP address from which you want to allow incoming traffic to originate. For practice, type `thisnetwork.org`.
4. Click **Add**. When you're brought back to the main window, click **Apply Policy**.

Highlight your new policy; the **Remove Rule** and **Edit Rule** buttons are now activated. Unless you created an actual rule that you plan to use, click **Remove Rule** and then **Apply Policy**.

You can also use Firestarter to block outbound traffic to a specific network, site, or host. Change the **Editing** setting to **Outbound traffic policy**; you can now select either **Permissive** or **Restrictive**. **Permissive** blacklists selected traffic; if you create a policy in Permissive mode, you're telling Firestarter to prevent outgoing traffic to anything listed in the policy. **Restrictive**, on the other hand, blocks any outgoing traffic *except* to those listed in the policy.

For example, if you want your computer to access only `www.thisnetwork.org`, select **Restrictive** and then click **Add Rule**. In the **Add new outbound rule** window, enter `www.thisnetwork.org` and then click **Add** followed by **Apply Policy**.

To block access to `www.thisnetwork.org`, select **Permissive** and click **Add Rule**. Again, type `www.thisnetwork.org` in the **Add new outbound rule** window, and then click **Add** and **Apply Policy**.

Once you've made policy changes to Firestarter, you can lock the firewall by clicking the **Status** tab and selecting **Lock Firewall**.

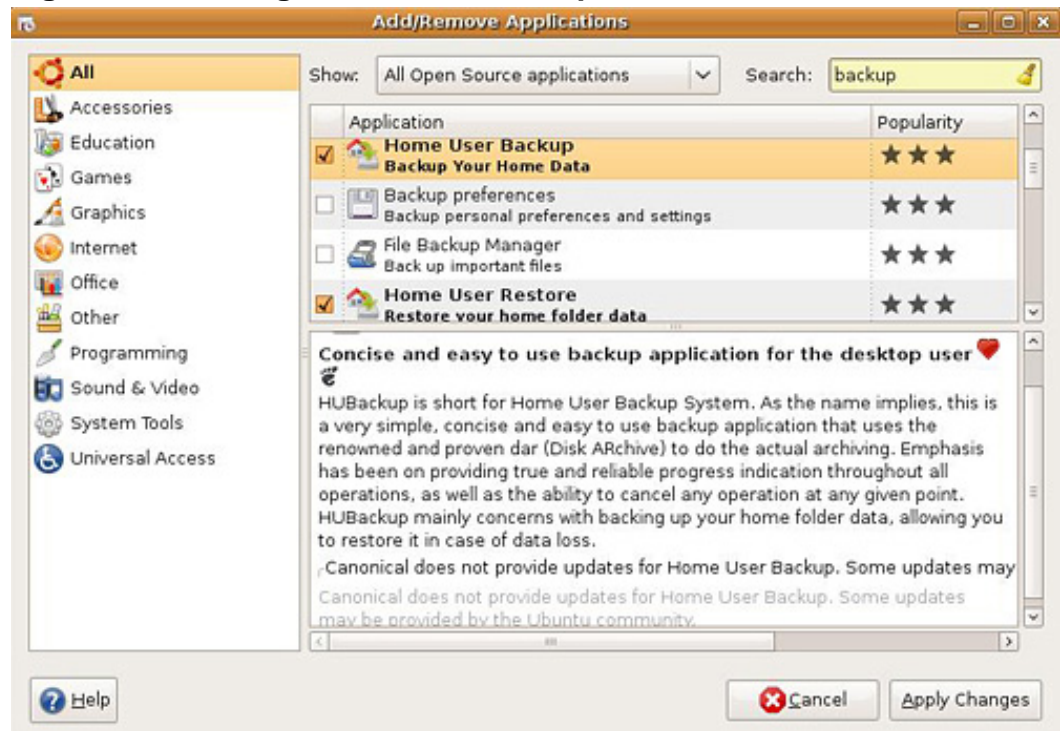
Section 5. Backing up and restoring desktop files

Another step in protecting your GNU/Linux desktop from disaster involves the backup and recovery process. Again, you install software from the Add/Remove tool; select **Applications > Add/Remove** to open the **Add/Remove Applications** window. Then, follow these steps:

1. Make sure the **Show** drop-down menu is set to **All Open Source applications**.
2. Type `backup` in the **Search** box, and press **Enter**. A list of software packages appears in the window.
3. Scroll down to the Home User Backup package, and select it.
4. The Add/Remove tool asks if you want to install bundled applications. This refers to the Home User Restore application; click **Install All**.
5. Select the **Home User Backup** and **Home User Restore** check boxes,

and then click **Apply Changes** (see Figure 8).

Figure 8. Installing Home User Backup and Home User Restore



6. Click **Apply** in the next window, and then enter your password and click **OK**.

Once you've installed the backup and restore software, you can access it by choosing **System > Administration > Home User Backup/Restore**. In the next section, you perform a backup of your home folder.

Perform a backup

Start Home User Backup. When the program is launched, you're given the option to back up all files in the home folder or back up a specific folder. The first time you back up anything, you should select the **All Files** option. Subsequently, when you make significant changes, you can then select specific folders to back up. (Many times, people choose to back up everything each time they run their backup program. Although this may seem to make sense, it's a huge waste of resources. Not only does the backup take up storage space, but backing up large amounts of data takes a while.)

Before you click the **Backup** button, you need to determine where to save the backup file. For obvious reasons, it's wise to back up to an attached storage drive rather than a folder on the computer.

Once you've selected your backup location, click the **Backup** button. Home Backup User asks if you want to verify the integrity of the data; this is a good option, because you'll have greater confidence that the backup file can be successfully restored if you need it. When you look at the files that were created, you'll see a master-archive file and a master-catalog file. Both have the extension .dar.

Restore data

Before you restore data from a backup, you need to first create a target folder where the files should be sent. It's a good option to create a folder on the desktop so you can easily access the restored files. After you create the target folder, launch the terminal to perform the actual restoration. At the prompt, type

```
sudo dar -x /path/archive_file -R /path/targetfolder
```

Press **Enter**, provide your password, and press **Enter** again. The restore process populates the target folder with the data contained in your backup file.

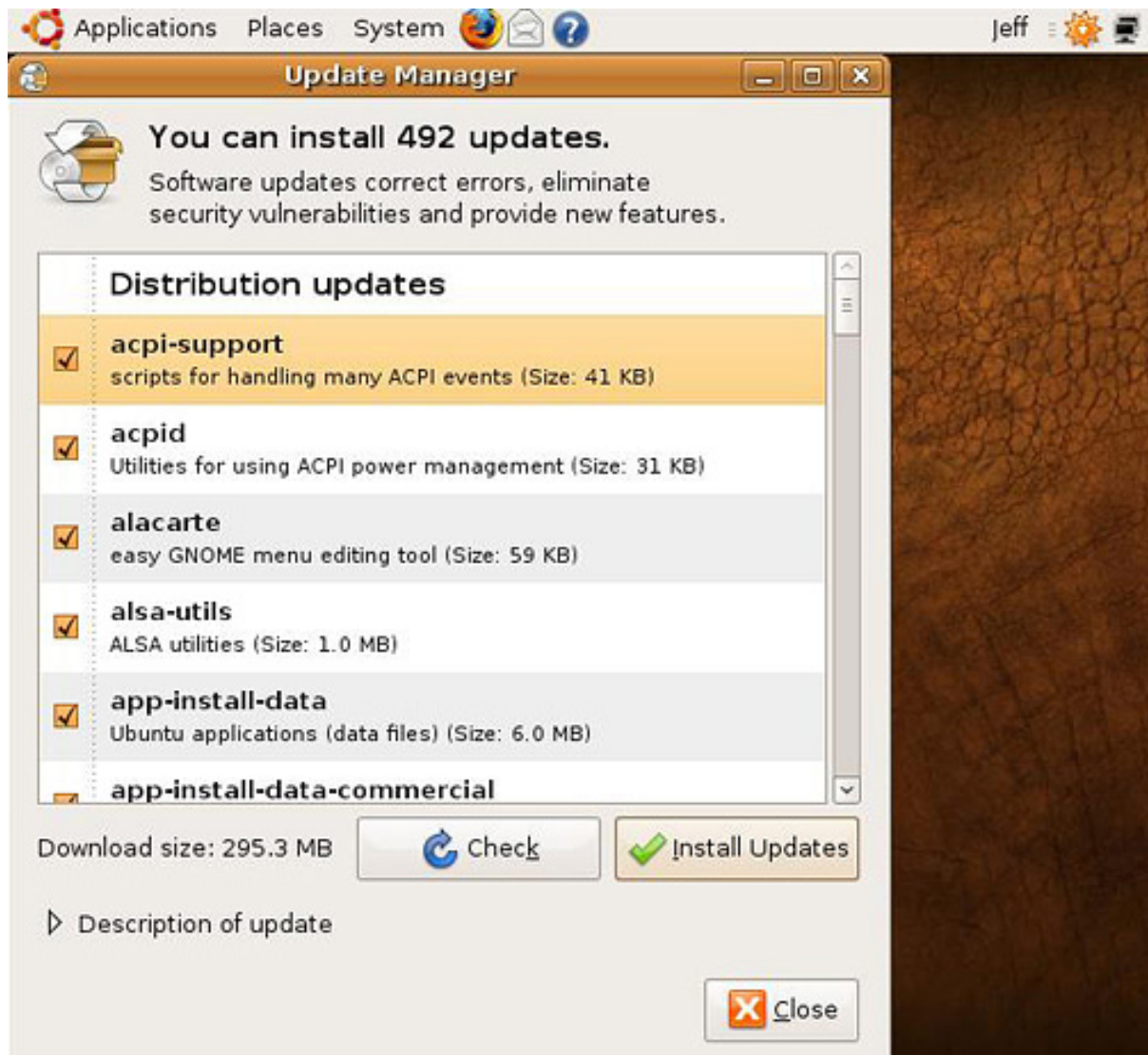
Section 6. Installing updates

Many attacks against computers are launched when a malicious hacker finds a vulnerability in the operating-system software or another piece of software the computer is running. When software (including operating systems) is released, it often contains multiple vulnerabilities that malicious hackers can exploit. Over time, software developers and security experts find these vulnerabilities and create patches and updates for the software to plug the holes.

As a computer user, it's essential for you to make sure your operating system and software are up to date. Most operating systems have a built-in feature that informs you when updates are available, and many of the GNU/Linux distributions include this functionality.

Ubuntu uses an orange icon on the menu bar of the desktop to alert you about new updates for all software maintained in the Ubuntu repositories. Clicking this icon brings up the **Update Manager** window in which you can select software for which to install updates (see Figure 9). Clicking **Install updates** begins the process. You're told what changes will be made and given an estimate of how long the update should take; you then have the option to cancel the update or continue installing any new packages. If any errors occur during the update, you're alerted.

Figure 9. Updating the operating system and other software



Section 7. Password-protecting the bootloader

When you're using GNU/Linux, you can boot the computer to change the root password without having to enter a password. This is called *single-user mode*, and in this section you password-protect this feature.

First you're going to password-protect the GRUB bootloader. If you're using LILO, follow these steps:

1. Open the terminal, type the command `grub` at the prompt, and press

Enter.

2. To make sure you don't store the password you're going to create in plaintext, enter the command `md5crypt` and press **Enter**.
3. The prompt asks for a password. Type the password you wish to use for single-user mode, and then press **Enter**.
4. You're given an encrypted version of the password. Don't close this terminal window -- you'll need this encrypted password shortly.

Edit the GRUB configuration file

Before you edit the GRUB configuration file, you need to back it up. Follow these steps:

1. Open a new terminal window, type the following command, and then press **Enter**: `sudo cp /boot/grub/menu.lst /boot/grub/menu.lst-backup`
2. You're asked for your password; enter it, and press **Enter** again.
3. Type the following command and press **Enter**: `gedit /boot/grub/menu.lst`
4. Press **Enter**. You're brought to the Grub configuration file. Locate the line in the file that reads `password md5 --` and change the existing entry in the GRUB configuration file with the encrypted password you created earlier in this section. Listing 1 shows what your GRUB configuration file should look like when the password has been changed:

Listing 1. GRUB configuration file, after the password change

```
# Set a timeout, in SEC seconds before automatically booting the default
entry
# (normally the first entry defined).
timeout          3

## hiddenmenu
# Hides the menu by default (press ESC to see the menu)
hiddenmenu

# Pretty colours
#color cyan/blue white/blue

## password ['--md5'] passwd
# If used in the first section of the menu file, disable all interactive
editing
# control (menu entry editor and command-line) and entries protected by the
```

```
# command 'lock'
# e.g. password topsecret
#     password --md5 $1$jLhUO/$aW78kHK1QfV3P2b2znUoe/
# password topsecret

#
# examples
#
# title           Windows 95/98/NT/2000
```

If you're using the LILO bootloader, open the terminal and edit `cat /etc/lilo.conf`. When the editor opens, search for the password section, and create a password there. Unlike GRUB, LILO doesn't allow for encrypted passwords.

Section 8. Conclusion

This tutorial has introduced a few tools that can help you harden your GNU/Linux desktop. It's important to note that even if you install all the tools available to protect your computer and the data stored within, ultimately you are responsible for using those tools. Set a schedule to check for updates to ClamAV and rkhunter. Make it a common practice to run these utilities on a weekly basis and whenever you install new software. Set a backup schedule for your data, and, most important, stay up to date on trends in computer security.

Resources

Learn

- In the [developerWorks Linux zone](#), find more resources for Linux developers (including developers who are [new to Linux](#)), and scan our [most popular articles and tutorials](#).
- See all [Linux tips](#) and [Linux tutorials](#) on developerWorks.
- Stay current with [developerWorks technical events and Webcasts](#).

Get products and technologies

- Download [Ubuntu](#) for use in the hands-on portion of this tutorial.
- Download [Sun VirtualBox](#) to create a virtual machine you can use to practice the lessons in this tutorial.
- [Order the SEK for Linux](#), a two-DVD set containing the latest IBM trial software for Linux from DB2®, Lotus®, Rational®, Tivoli®, and WebSphere®.
- With [IBM trial software](#), available for download directly from developerWorks, build your next development project on Linux.

Discuss

- Get involved in the [developerWorks community](#) through blogs, forums, podcasts, and spaces.

About the author

Jeffrey Orloff

Jeffrey Orloff serves as the Director of IT and Security for SafeWave, LLC. He also works as the technology coordinator for the School District of Palm Beach County's Department of Alternative Education/DJJ.

Trademarks

IBM, the IBM logo, ibm.com, DB2, developerWorks, Lotus, Rational, Tivoli, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law

trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. See the current list of [IBM trademarks](#).

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Windows is a trademark of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.