Hardening the Linux desktop

An introduction to GNU/Linux desktop security

Jeffrey Orloff
Director of IT/Security
SafeWave, LLC

05 February 2014
(First published 12 December 2008)

Although GNU/Linux® has the reputation of being a much more secure operating system than Windows,® you still need to secure the Linux desktop. This article steps you through installing antivirus software, creating a backup and restore plan, and using a firewall so you can harden your Linux desktop against most attacks and prevent unauthorized access to your computer.

Introduction

Malicious attacks against computers are on the rise. Although fewer viruses have been written to attack GNU/Linux systems than Windows systems, GNU/Linux viruses do exist. Furthermore, the amount of other types of malware that can infect a computer running Linux — as well as the sheer number of attacks — are growing. Recently Wirenet.1 attacked computers running Linux and Mac OS X. The malware stole passwords and other information stored in the computer's Internet browser, email client, and instant messaging tool.

How myths about security grow

When mischief was the focus for malicious hackers, Windows systems were the primary target because they were easy to use and many novice users bought them. Some attacks were motivated by the desire to bring negative publicity to Microsoft, which was perceived as not supporting the open source community. These attacks fostered myths in computing circles that Windows security was weak.

Platform-independent environments such as OpenOffice.org, Perl, and Mozilla Firefox are not exempt. For example, Dropper.MsPMs, a malicious Java archive (JAR) file, was found on machines running Windows, Mac OS X, and Linux.

Some malware packages are written specifically for GNU/Linux. A *rootkit*— a collection of tools that let an attacker gain access to the root (administrator) account on your computer — are part of the same software family as Trojan horses. These malware packages go by different names such as tOrn and ARK.

Protecting against malware

Many factors determine how secure a system is, but the most important is how the system is configured. This article addresses the configuration of the GNU/Linux desktop. By taking the steps to configure your computer system properly, you can make sure it's secure. The place to start is with anti-virus protection.

Install antivirus protection: ClamAV

ClamAV is an open source (GPL) antivirus engine designed for detecting Trojans, viruses, malware, and other malicious threats. When installing it, you can specify whether you want to run the program manually or have it run continually by connecting it to a daemon. For a desktop, running the program as a daemon is ideal because you still have the option of performing manual scans.

To install ClamAV as a continually running daemon, perform these steps:

1. Power up your computer and log in.
2. From the menu bar, click **Applications > Accessories > Terminal**.
3. When the terminal is launched, enter the following command:
   ```
   sudo apt-get install clamav-daemon
   ```
4. When prompted, enter your password.
   Doing so installs a package called `clamav-freshclam`, which is the updater package for the ClamAV application.
5. You now see a message indicating how much disk space will be used when you install the software. Enter `Y` at the prompt to begin installation.
   The installation process should take only a couple of minutes. When it finishes, you see an alert indicating that your virus database is older than *x* days and that you should update it using the next series of steps.
6. At the prompt, run the command `sudo freshclam`.

Running `freshclam` updates your virus definitions to the latest release. Keeping your definitions up-to-date is important, because this is how ClamAV identifies malware.

Virus definitions are patterns of code unique to malware programs. Antivirus scanners compare the contents of your files to the code patterns in a virus definitions database. If a match is found, the program alerts you that an infected file resides on your computer and prevents code in that file from executing.

If the definition for a particular piece of malware isn't in your virus definitions database, the antivirus scanner won't know it's malicious code and lets it run and do whatever damage it was programmed to do. Update your definitions on a regular basis to provide the most comprehensive protection you can.

Starting ClamAV

ClamTk: A GUI for your antivirus application

If you don't like working from the terminal, you can opt to install a GUI for ClamAV called ClamTk. This GUI is easy to install using the Add/Remove Applications tool in Ubuntu. Once installed, run it by clicking **Applications > System Tools > Virus Scanner**.

Now that you've updated your virus definitions, you're ready to start ClamAV. To run a manual scan of your home folder, go to the terminal prompt and enter `clamscan`. When the `clamscan` command finishes, you see a report of how many directories and files were scanned and how many infected files were found.

~~To run ClamAV as a daemon, go to the terminal prompt and enter `clamdscan`. The `clamdscan` command creates a user named ClamAV. You can then add this user to the group that owns the files you want to scan.~~

Protect against rootkits with rkhunter

Probably the most dangerous malware that GNU/Linux users face is the rootkit. The Rootkit Hunter (`rkhunter`) and `chkrootkit` programs scan your desktop for suspicious files that an attacker may have installed to gain control of your computer.

To install `rkhunter`, one of the best programs for finding and removing rootkits, perform these steps:

1. To navigate back into the terminal, click **Applications > Accessories > Terminal**.
2. In the terminal shell, enter the following command:

```
~~sudo aptitude install rkhunter~~ sudo apt-get install rkhunter
```

3. When you receive a message informing you of how much space the software will use, enter `Y` to begin installation.

When `rkhunter` has been installed, you can run it to check your desktop for exploits. Go to the terminal prompt and enter `sudo rkhunter --check`.

If `rkhunter` is running properly, you see a list of directories with the word `OK` or `Warning` next to them. When started, `rkhunter` performs several types of scans. After one scan finishes, begin the next by pressing **Enter**. The types of scans are:

- Directories
- Exploits on the desktop
- Ports that are commonly used for backdoor access
- Startup files, groups and accounts, system configuration files, the file system
- Applications

After all the scans are complete, `rkhunter` provides you with a report and creates a log file with the results.

As with ClamAV, you need to update `rkhunter` regularly so that it can detect the latest vulnerabilities and exploits:

1. From the terminal, enter `sudo rkhunter --update`.
2. When prompted, enter your password.

Use Tiger to scan your system

In terms of security, establishing a baseline is one of the most important things you can do. From there, you can tell if anything has been tampered with, because it alters the baseline. If you install an office productivity suite, you also alter the baseline, but you approved that addition. If a piece of malware is installed to your machine, a check against the baseline should reveal this, as well.

Most people don't have any idea how to manually create a baseline of their computer's configuration. However, a program called Tiger audits the computer system to see whether anything has been altered. If it has, the software provides an error code.

To install Tiger on your Ubuntu desktop, start by opening the terminal. From there, run the following command:

```
sudo aptitude -y install tiger
```

sudo apt-get install tiger

That command puts the software on your machine. Now, you need to run it.

With the terminal still open, run `sudo tiger` to create a report of security issues, and save that report to /var/log/tiger. The name of the file often contains the computer's hostname followed by the date and time — for example, `security.report.hostname.121220-8:46`. The name of the file is provided to you when the report is complete.

To view the report, run `sudo gedit` and include /var/log/tiger and the file name. Using this example, the command is:

```
sudo gedit /var/log/tiger/security.report.hostname.121220-8:46
```

The report then provides error codes for the problems it finds. You can find the meaning of each error code online (see Resources).

Using a firewall

The next preventative step you should take is to use the firewall built into your operating system. Ubuntu, by default, runs `iptables` as the firewall on every distribution. Upon installation, the default settings for this firewall allow all incoming and outgoing traffic. To make effective use of the firewall, you need to create rules to lock down your desktop.

You can configure `iptables` through the terminal, but you can also write firewall rules with a GUI called Gufw based on the Uncomplicated Firewall (UFW) program that comes with Ubuntu.

Install Gufw by opening the terminal and running the following command:

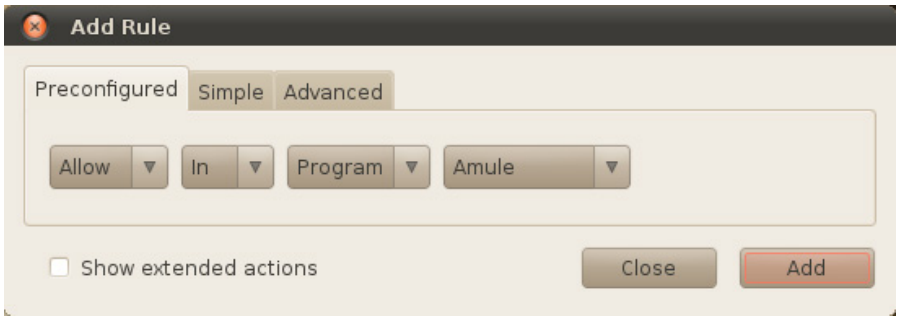
```
sudo apt-get install gufw
```

When the installation is complete, you can access it from **System >Administration > Firewall**. When opened, enable Gufw, which is disabled by default. Under the heading **Actual Status**, click the **Enabled** check box to turn it on. Doing so sets all incoming traffic to **Deny**. Then click **Add** to create rules according to how you want UFW to handle certain types of traffic based on the four available options:

- **Allow.** The system allows entry traffic for a port.
- **Deny.** The system denies entry traffic to a port.
- **Reject.** The system denies entry traffic to a port and informs the requesting for connection system that it has been rejected.
- **Limit.** The system denies connections if an IP address has attempted to initiate six or more connections in the past 30 seconds.

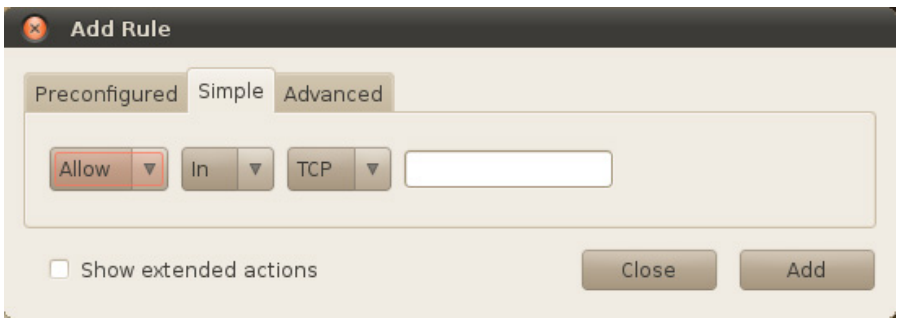
When you click **Add**, a window appears with three tabs: **Preconfigured**, **Simple**, and **Advanced**. The **Preconfigured** tab is the easiest way to create rules, because you select what you want to allow or deny from a drop-down list, as shown in Figure 1:

Preconfigured rules



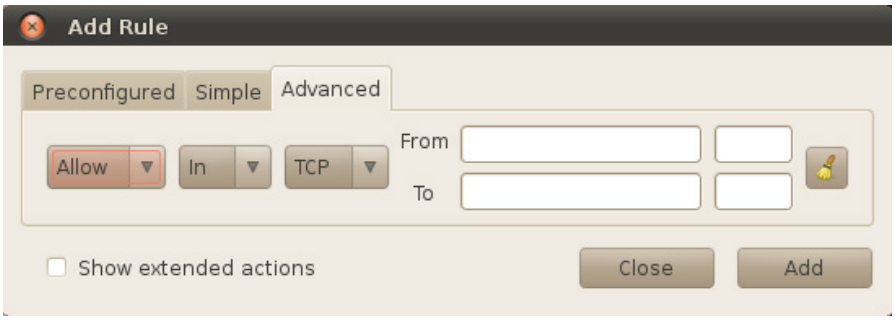
With the **Simple** tab, you can tell UFW whether you want to allow or deny something and then select the protocol/service and port number. See Figure 2:

Simple rules



You can fine-tune the rule even further with the **Advanced** tab. See Figure 3:

Advanced rules



Backing up and restoring desktop files

Another step in protecting your GNU/Linux desktop involves establishing a backup and recovery process.

At one time you had to install backup and recovery software in most Linux distributions. However, the need to have a sound disaster recovery solution prompted many to include some sort of backup and recovery software in the installation. Ubuntu relies on Duplicity, a program that uses `rsync`. To make things even easier, Ubuntu comes with Deja Dup, a graphical front end to Duplicity.

To get started with Deja Dup, click **System Settings** from the gear icon. In the **System Settings** window, click **Backup**.

Backups

Storage location

Before you turn on automatic backups, click **Storage** to set the backup location. You can use Ubuntu One (a cloud storage option), send your backups to another server through FTP, save to a local folder, or set a custom location. When you determine the best location for your backup files, click **Folders** to select what you want to back up. You have two options here: **Folders to back up** and **Folders to ignore**. You can add or delete any folders from either column.

Now, click **Schedule** to tell Deja Dup how often to run your backups and how long to keep them. You can opt to back up daily, weekly, biweekly, or monthly, and these backups can be stored for at least one week to at least one year or even forever.

Now, go back to **Overview** and slide **Automatic backups** to **On**. That's all it takes. If you ever need to restore files, click **Restore**, and Deja Dup will ask you from where you want to restore, from what date, and to what location you would like to restore your files. It's a good idea to make sure your backups are working properly by restoring files every now and again.

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. Security experts look for these vulnerabilities and create software patches and updates to plug the holes.

Keep your software 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 type of functionality. Click the gear icon on the menu bar of the desktop, then click **Software Up to Date**

Software & Updates

to launch the Update Manager. The Update Manager usually opens on its own when new updates are available.

In the Update Manager window, you can click **Install Updates**. You can also choose how often and what software you want to update by clicking **Settings**. The default options should be good as long as the **Important security updates** check box is selected and the **When there are security updates** option is set to **Download and install automatically**.

Password-protecting the bootloader

When you use GNU/Linux, you can boot the computer to change the root password without having to enter a password. This is called **single-user mode**. To password-protect this feature, you have two bootloader options: GRUB and LILO. If you use GRUB, you can encrypt your password to make things even more secure. Users of LILO do not have this option. If you use GRUB, perform these steps:

1. Launch the terminal.
2. At the prompt, enter `grub`.
3. To make sure you don't store the password you're going to create in plain text, enter `md5crypt`.
4. At the prompt, enter the password you want to use for single-user mode. You are then given an encrypted version of the password. Don't close this terminal window — you'll need this encrypted password in the next steps.

Now, you need to edit the GRUB configuration file. Of course, back it up first:

1. Enter the following command:
```
sudo cp
                    /boot/grub/menu.lst /boot/grub/menu.lst.backup
```
2. When prompted, enter your password.
3. Enter the following command:
```
gedit /boot/grub/menu.lst
```
   This takes you to the GRUB configuration file.
4. Locate the line in the file that reads `password --md5` and replace the existing password with the encrypted password you created earlier.
   Listing 1 shows what your GRUB configuration file should look like when the password has been changed:

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 $1$jLhU0/$aW78kHK1QfV3P2b2znUoe/ #
                    password topsecret # # examples # # title Windows 95/98/NT/2000
```

~~Unlike GRUB, LILO doesn't allow for encrypted passwords. If you're using the LILO bootloader, perform these steps:~~

~~1. Launch the terminal.~~
~~2. At the prompt, enter `edit cat /etc/lilo.conf`.~~
~~3. When the editor opens, search for the password section and create a new password there.~~

Conclusion

This article has introduced a few tools that can help you harden your GNU/Linux desktop. Even if you install all the tools available to protect your computer and the data stored on it, ultimately, you're responsible for using those tools.

Set a schedule to check for updates to ClamAV and `rkhunter`. Run these utilities weekly 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. New vulnerabilities are discovered constantly. Stay informed and take appropriate action to maintain the security of your computer.

Resources

Learn

- "Secure Linux containers cookbook" (Serge E. Hallyn, developerWorks, 2009): Learn how to strengthen lightweight containers with SELinux and Smack.
- "Secure Linux: Part 1" (Evgeny Ivashko, developerWorks, 2012): Learn about the basic milestones in the development, architecture, and operating principles of Security-Enhanced Linux.
- "Anatomy of Security-Enhanced Linux (SELinux)" (M. Tim Jones, developerWorks, 2012): Learn more about the architecture and implementation of SELinux.
- developerWorks Linux zone: Find more resources for Linux developers (including developers who are new to Linux).
- Stay current with developerWorks technical events and webcasts focused on a variety of IBM products and IT industry topics.
- Follow developerWorks on Twitter.
- Watch developerWorks on-demand demos ranging from product installation and setup demos for beginners, to advanced functionality for experienced developers.

Get products and technologies

- Download Ubuntu Desktop Edition to follow along with the lessons in this article.
- Learn more about UFW from the Ubuntu wiki.
- Learn more about Tiger, security audit and intrusion-detection tool.
- Learn more about ClamAV to help protect your computer from malware.
- Learn more about how Rootkit Hunter can help secure your computers.
- Learn more about iptables from the Ubuntu wiki.
- Learn more about Duplicity and Deja Dup.
- Evaluate IBM products in the way that suits you best: Download a product trial, try a product online, or use a product in a cloud environment.

Discuss

- Get involved in the My developerWorks community. Connect with other developerWorks users while exploring the developer-driven blogs, forums, groups, and wikis.

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.