

By Kirk R. Halyk

## Takeaway

No matter which Linux distribution you choose, there are at least 10 things you do to properly prepare the operating system for connection to the Internet.

---

## 10 things before the Internet

*Editor's note: As part of a recent [IT Soapbox](#) blog post I asked Linux users and evangelists in the TechRepublic community to step up to the plate and take a crack at producing some informative articles and downloads on the Linux operating system. This document is just one of the submissions inspired by that challenge. Just click the [Linux challenge](#) tag to track other published submissions stemming from this grass roots project.*

### 1: Your purpose

Linux, like Microsoft Windows, is simply a computer operating system. When I talk to friends or co-workers who are embarking on the Linux experience for their initial time, this is the first point I stress. Linux in itself is not a magic wand that can be waved and make all sorts of computing problems disappear. While Windows has its own set of problems, so too does Linux. There is no such thing as a perfect or completely secure computer operating system. Will the machine be a desktop computer or a server; purpose is a key to understanding how to initially install and configure your Linux PC.

### 2: Installation

Unlike Windows, Linux does not present itself as a "server" version or as a "desktop" version. During a typical installation of Linux the choice is yours as to exactly what software you wish to install and therefore exactly what type of a system you are constructing. Because of this, you need to be aware of the packages that the installation program is installing for you. For example, some distributions will configure and start a Samba server or a mail server as part of the base install. Depending upon the purpose of your Linux PC and the security level you are prepared to accept, these services may not be needed or desired at all. Taking the time to familiarize yourself with your distributions' installer can prevent many headaches and/or reinstalls down the road.

### 3: Install and configure a software firewall

A local software firewall can provide a "just in case" layer of security to any type of network. These types of firewalls allow you to filter the network traffic that reaches your PC and are quite similar to the Windows Firewall. The [Mandriva](#) package called [Shorewall](#) along with a component of the Linux kernel called *Netfilter* provides a software firewall. By installing and configuring Shorewall during the installation process, you can restrict or block certain types of network traffic, be it coming to or going out from your PC.

To access and configure your firewall for Mandriva simply run the *mcc* (or Mandriva Control Center) command from a command prompt or, depending upon your graphical environment, you may be able to access the Mandriva Control Center from your base system menu. In the security options, select the firewall icon and you will be presented with a list of common applications that may need access through your firewall. For example, checking the box for "[SSH server](#)" will open port 22 needed by the Secure Shell server for secure remote access. There is also an advanced section which will allow you to enter some less commonly used ports. For example, entering "8000/tcp" will open port 8000 on your PC to TCP-based network traffic.

Blocking or allowing network traffic is one layer of security, but how do you secure a service that you do allow the Internet or your intranet to connect to? Host based security is yet another layer.

### 4: Configuring the */etc/hosts.deny* and */etc/hosts.allow* files

In the preceding section we looked at the example of opening the Secure Shell service to network traffic by opening port 22 on our firewall. To further secure this server from unwanted traffic or potentially hackers, we may wish to limit the hosts or computers that can connect to this server application. The */etc/hosts.deny* and */etc/hosts.allow* files allow us to do just that.

When a computer attempts to access a service such as a secure shell server on your new Linux PC the */etc/hosts.deny* and */etc/hosts.allow* files will be processed and access will be granted or refused based on some easily configurable rules. Quite often for desktop Linux PC's it is very useful to place the following line in the */etc/hosts.deny* file:

```
ALL: ALL
```

This will deny access to all services from all hosts. It seems pretty restrictive at first glance, but we then add hosts to the */etc/hosts.allow* file that will allow us to access services. The following are examples that allow some hosts remote secure shell access:

```
sshd: 192.168.0.1          #allow 192.168.0.1 to access ssh
sshd: somebox.somedomain.com #allow somebox.somedomain.com to access ssh
```

These two files provide powerful host based filtering methods for your Linux PC.

### 5: Shutoff or remove non-essential services

Just like Windows there can be services running in the background that you either don't want or don't have a purpose for. By using the Linux command *chkconfig* you can see what services are running and turn them on and off as needed. Services that are not running don't provide security holes for potential hackers and don't take up those precious CPU cycles.

### 6: Secure your required services

If your new Linux PC has some services that will receive connections from the Internet make sure you understand their configurations and tune them as necessary. For example, if your Linux PC will receive secure shell connections make sure you check the *ssh config* file (for Mandriva it is */etc/ssh/sshd\_config*) and disable options like root login. Every Linux PC has a root user so you should disable root login via *ssh* in order to dissuade brute force password crack attempts against your super-user account.

## **7: Tune kernel networking security options**

The Linux kernel itself can provide some additional networking security. Familiarize yourself with the options in the `/etc/sysctl.conf` file and tune them as needed. Options in this file control, for example, what type of network information is logged in your system logs.

## **8: Connect the PC to a router**

A hardware router is a pretty common piece of household computer hardware these days. This is the front line security to any home or business network and provides multiple PC's to share one visible or external Internet address. This is generally bad news for any hacker or otherwise malicious program that may take a look at your new Linux PC as it blocks any and all network traffic that you don't specifically allow. Home networking routers are just smaller versions of what the big companies use to separate their corporate infrastructure from the Internet.

## **9: Update**

Always keep the software on your computer up to date with the latest security patches should you be running Linux, Windows, BSD or WhoKnowsWhat. Your distribution will release regular security patches that should be applied and are available off the Internet. As with Windows, this should always be your first Internet destination.

## **10: Other software**

Your second Internet stop may be to install some other hardening or system monitoring software.

[Bastille-Linux](#) is a program that can be used to "harden" or secure certain aspects of your new Linux PC. It interactively develops a security policy that is applied to the system and can produce reports on potential security shortcomings. On top of that it is a great tool to use for learning the in and out of securing your Linux PC.

[Tripwire](#) is a software package that monitors your system binaries for unauthorized modifications. Often a hacker may modify system binaries that may be useful in detecting a system intrusion. The modified programs would then report false information to you allowing the hacker to maintain his control over your system.

## Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for our [Downloads Weekly Update](#) newsletter
- Sign up for TechRepublic's [Linux NetNote](#) newsletter
- Check out all of TechRepublic's [free newsletters](#)
- [10 things you should do to prepare every new Linux installation](#)
- [10 things you should know about every Linux installation and distro](#)

## Version history

**Version:** 1.0

**Published:** December 8, 2005

## Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team