Preface

Hack Proofing Linux: A Guide to Open Source Security is designed to help you deploy a Linux system on the Internet in a variety of security roles. This book provides practical instructions and pointers concerning the open source security tools that we use every day.

First, we show you how to obtain the software; and then, how to use the Bastille application to "harden" your Linux operating system so that it can function securely as it fulfills a specific role of your choice (e.g., as a Web server, as an E-mail server, and so forth). You will also learn how to use your Linux system as an auditing tool to scan systems for vulnerabilities as well as create an Intrusion Detection System (IDS), which enables your Linux system to log and respond to suspicious activity. From virus protection to encrypting transmissions using Gnu Privacy Guard and FreeSWAN, you will be able to configure your system to secure local data as well as data that will be passed along the network. After reading this book, you will be able to identify open source and "for-fee" tools that can help you further secure your Linux system.

We have also included chapters concerning ways to sniff and troubleshoot network connections and how to implement strong authentication using One Time Passwords (OTP) and Kerberos. Tools such as Squid proxy server and Ipchains/Iptables will help you use your Linux system so that it can act as a firewall. With the tools on the accompanying CD as well as the advice and instructions given in this book, you will be able to deploy your Linux system in various roles with confidence.

We decided to focus on profiling the most commonly used security tools found on the Linux platform. We also decided to emphasize the real-world implementation of these tools, as opposed to just providing conceptual overviews. Finally, we decided to describe the steps you should take when things go wrong. As a result, we have created a book that is a valuable resource that helps you use your Linux system as efficiently as possible.

One of the most exciting things about this book is that it provides hands-on instructions for implementing security applications. From Gnu Privacy Guard (GPG) and Bastille to FreeSWAN, Kerberos, and firewall troubleshooting utilities, this book shows you how to use your Linux skills to provide the most important security services such as encryption, authentication, access control, and logging.

While writing the book, we had the following three-part structure in mind:

- Locking Down the Network (Chapters 1 through 4)
- Securing Data Passing Across the Network (Chapters 5 through 8)
- Protecting the Network Perimeter with Firewalls (Chapters 9 through 11)

Each of these sections is designed to help you find the best solution for your particular situation. Although the book itself isn't explicitly divided into sections, as you are reading remember this rough division because it will help you to implement security measures in your own environment.

Chapter 1 discusses open source concepts, including the GNU General Public License, as presented by the www.gnu.org people (the Free Software Foundation), and then moves on to showing how you can use GPG and Pretty Good Privacy (PGP) to encrypt transmissions and also to check the signatures of files that you download from the Web. It also provides information concerning the steps to take when auditing a network.

Chapter 2 shows you how to lock down your operating system so that it provides only those Internet services that you desire. Chapter 3 shows you how to use applications such as AntiVir, Gnome ServiceScan, Nmap, Rnmap, and Nessus to scan for vulnerabilities. In Chapter 4, you will learn about host and network-based IDS applications such as Snort, Tripwire, and PortSentry. Chapter 5 explains how to use network sniffers such as Tcpdump, Ethereal, and EtherApe to their full advantage. With this knowledge, auditing a network and truly understanding what is going on "beneath the hood" will make you a much more effective network security administrator.

By the time you finish Chapter 6, you will know how to deploy One Time Passwords and Kerberos, and in Chapter 7, you will understand how to avoid sniffing attacks, and in Chapter 8, you will enable IPSec by deploying FreeSWAN. Chapter 9 empowers you to create personal firewalls as well as packet filtering firewalls using either Ipchains or Iptables. Chapter 10 shows you how to implement Squid so that you can more carefully monitor and process packets. Finally, Chapter 11 provides you with tools that test your firewall implementation.

The open source community has fulfilled the need for a powerful, free system that allows you to conduct audits, serve up Web pages, provide e-mail services, or any other Internet service you wish to provide. Once you are able to take advantage of the security software provided by the open source community, you will receive the benefit of having a huge pool of developers working for you. You will gain more freedom because you will be able to choose widely tested security tools provided by a variety of skilled developers. You can even choose (at your own risk) to use rather obscure tools that have been recently created. It is up to you.

Open source operating systems and security tools are both a blessing and a curse: You are blessed with (usually) free software, but you are then cursed with having to spend time working with the software's idiosyncrasies. By reading this book and implementing the tools and practices we've described, you should be able to minimize the "curse." It is also our hope that as you read this book you will also become further involved in the open source software movement, which has begun to fulfill its promise of creating powerful, useful software.

—James Stanger, Ph.D., MCSE, MCT