SYNGRESS®

1 YEAR UPGRADE
BUYER PROTECTION PLAN

HACK PROOFING™ LINUX

Your Guide to Open Source Security

- Step-by-Step Instructions for Deploying Open Source Security Tools
- Hundreds of Tools & Traps and Damage & Defense Sidebars, Security Alerts, and Exercises!
- Bonus Wallet CD with Configuration Examples, Packet Captures, and Programs

James Stanger, Ph.D.
Patrick T. Lane
Edgar Danielyan Technical Editor

Global Knowledge
RECOMMENDED READING

solutions@syngress.com

With more than 1,500,000 copies of our MCSE, MCSD, CompTIA, and Cisco study guides in print, we continue to look for ways we can better serve the information needs of our readers. One way we do that is by listening.

Readers like yourself have been telling us they want an Internet-based service that would extend and enhance the value of our books. Based on reader feedback and our own strategic plan, we have created a Web site that we hope will exceed your expectations.

Solutions@syngress.com is an interactive treasure trove of useful information focusing on our book topics and related technologies. The site offers the following features:

- One-year warranty against content obsolescence due to vendor product upgrades. You can access online updates for any affected chapters.
- "Ask the Author"™ customer query forms that enable you to post questions to our authors and editors.
- Exclusive monthly mailings in which our experts provide answers to reader queries and clear explanations of complex material.
- Regularly updated links to sites specially selected by our editors for readers desiring additional reliable information on key topics.

Best of all, the book you're now holding is your key to this amazing site. Just go to **www.syngress.com/solutions**, and keep this book handy when you register to verify your purchase.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there's anything else we can do to help you get the maximum value from your investment. We're listening.

www.syngress.com/solutions

SYNGRESS®

The Only Way to Stop a Hacker Is to Think Like One

James Stanger
Patrick T. Lane

SYNGRESS®

KEY	SERIAL NUMBER
001	NFKA4UR934
002	DFTGEGHFG6
003	9456VMPDSP
004	MKC8EWR535
005	ZL94V343BB
006	AS56J89HGE
007	MJTY3D29H6
008	ADQW9UU6NN
009	5TGBXDQ7TN
010	KRF4W2F6P9

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Hack Proofing Linux: A Guide to Open Source Security

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN: 1-928994-34-2

Technical Editors: Edgar Danielyan and Larry Karnis
Co-Publisher: Richard Kristof
Acquisitions Editor: Catherine B. Nolan
Developmental Editor: Kate Glennon
CD Production: Michael Donovan
Freelance Editorial Manager: Maribeth Corona-Evans
Cover Designer: Michael Kavish
Page Layout and Art by: Shannon Tozier
Copy Editor: Beth A. Roberts and Darren Meiss
Indexer: Jennifer Coker

Distributed by Publishers Group West in the United States.

Acknowledgments

We would like to acknowledge the following people for their kindness and support in making this book possible.

Richard Kristof and Duncan Anderson of Global Knowledge, for their generous access to the IT industry's best courses, instructors, and training facilities.

Ralph Troupe, Rhonda St. John, and the team at Callisma for their invaluable insight into the challenges of designing, deploying and supporting world-class enterprise networks.

Karen Cross, Lance Tilford, Meaghan Cunningham, Kim Wylie, Harry Kirchner, Bill Richter, Kevin Votel, and Kent Anderson of Publishers Group West for sharing their incredible marketing experience and expertise.

Mary Ging, Caroline Hird, Simon Beale, Caroline Wheeler, Victoria Fuller, Jonathan Bunkell, and Klaus Beran of Harcourt International for making certain that our vision remains worldwide in scope.

Anneke Baeten, Annabel Dent, and Laurie Giles of Harcourt Australia for all their help.

David Buckland, Wendi Wong, Daniel Loh, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Charlotte Chan, and Joseph Chan of Transquest Publishers for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

Ethan Atkin at Cranbury International for his help in expanding the Syngress program.

Joe Pisco, Helen Moyer, Paul Zanoli, Alan Steele, and the great folks at InterCity Press for all their help.

Philip Allen at Brewer & Lord LLC for all his work and generosity.

Contributors

Patrick T. Lane (MCSE, MCP+I, MCT, Network+, i-Net+, CIW) is a Content Architect for ProsoftTraining.com, a leading Internet skills training and curriculum development company. He is the author of more than 20 technical courses and is the Director of the CIW Foundations and CIW Internetworking Professional series. While at ProsoftTraining.com, Patrick helped create the Certified Internet Webmaster (CIW) program and the i-Accelerate program for Intel, Novell, and Microsoft professionals.

Patrick consults as a mail, news, FTP, and Web Administrator for several organizations, including jCert Initiative Inc. and ProsoftTraining.com. He is also a network security consultant and writer who specializes in TCP/IP internetworking, LAN/WAN solutions, network and operating system security, and the Linux and Windows NT/2000 platforms. He has consulted for the University of Phoenix/Apollo Group, Novell, Intel, NETg, WAVE technologies, KT Solutions, SmartForce, and Futurekids. Patrick is a member of the CompTIA Network+ Advisory Committee, and co-author of Syngress Publishing's *E-mail Virus Protection Handbook* (ISBN: 1-928994-23-7). His work has been published in eight languages and he has been a featured speaker for the SmartForce Seminar Series on E-Business, the Internet World PING Series on Internet Protocol version 6, and the Information Technology Association of America (ITAA). He holds a master's degree in education.

James Stanger (Ph.D., MCSE, MCT) directs the Linux, Security, and Server Administrator certification tracks for ProsoftTraining.com. Since receiving his Ph.D. in 1997, he has focused on auditing Internet servers and writing courseware, books, and articles about administering and securing Internet servers. James has consulted for IBM, Symantec, Evinci

(www.evinci.org), Pomeroy (www.pomeroy.com), Securify (www.securify.com), Brigham Young University, and California State, San Bernardino. He specializes in troubleshooting firewalls, intrusion detection, DNS, e-mail, and Web server implementations.

James was the Technical Editor of Syngress Publishing's *E-mail Virus Protection Handbook* (ISBN: 1-928994-23-7) and has been an instructional designer of security and A+ courses for NetG, Thompson/WAVE learning, and ComputerPREP. Active in the Linux community, James sits on the Linux Professional Institute (www.lpi.org), SAIR (www.linuxcertification.org), and CompTIA Linux+ (www.comptia.org) advisory boards, each of which is dedicated to creating and maintaining industry-respected certifications. As the Vice Chair of the Linux Professional Institute (LPI) Advisory Council, he acts as liaison between the LPI and companies such as IBM, Compaq, and Intel.

Technical Editors

Edgar Danielyan (CCNA) is a self-employed developer specializing in GCC, X Window, Tcl/Tk, logic programming, Internet security, and TCP/IP; as well as having with BSD, SVR4.2, FreeBSD, SCO, Solaris, and UnixWare. He has a diploma in company law from the British Institute of Legal Executives as well as a paralegal certificate from the University of Southern Colorado. He is currently working as the Network Administrator and Manager of a top-level Armenian domain. He has also worked for the United Nations, the Ministry of Defense of the Republic of Armenia, and Armenian national telephone companies and financial institutions. Edgar speaks four languages, and is a member of ACM, IEEE CS, USENIX, CIPS, ISOC, and IPG.

Larry Karnis (RHCE, Master ACE, CITP), is a Senior Consultant for Application Enhancements, a Unix, Linux, and Internet consulting firm located in Toronto, Canada. His first exposure to Unix was over 20 years ago where he used Unix Version 6 while completing a bachelor's degree in computer science and mathematics. Larry deploys and manages Linux-based solutions such as Web and file and print servers, and Linux firewalls.

About the CD

This book is accompanied by a CD containing files and open source programs used throughout the book. The files include configuration examples, packet captures, and additional resources. We have included the specific open source programs used in the book so you can follow the chapter demonstrations step-by-step on your own systems.

Each file on the CD is discussed in detail and referenced throughout the book with the CD icon below. When a specific file or program is required, it directs you to the accompanying CD. The book also directs you to the Web site where you can download the most current version, and find additional resources relating to that program. For instance, you can download Free Secure Wide Area Network (FreeS/WAN) at www.freeswan.org, or use the version located on the CD. It is recommended that you use the version included on the CD because this will increase the chances that the book demonstrations will be successful, as some of the programs may have changed since this book was printed.

The book is written to Red Hat Linux 7.x. Therefore, most of the CD files are Red Hat Package Manager (.rpm) files. There are also many Tape Archive (.tar) files and GNU Zip (.gzip) files. Instructions for unpacking and installing these files are included in their respective locations throughout the book. To mount the CD onto your Linux system, you would issue the following command (for Red Hat systems):

```
mount -t iso9660 /dev/cdrom /mnt/cdrom
```

And to unmount:

```
umount /mnt/cdrom
```

It is recommended that you copy the CD files to your hard drive before working with them. If you use other versions of Linux, you may need to modify the demonstrations, or download a portable version of the open source programs to work with your version of Linux.

Look for this CD icon when obtaining files used in the book demonstrations.

Contents

Using the GNU General Public License

The GNU General Public License (GPL) is the basis of the open source movement. This license is provided by the Gnu is Not Unix (GNU) organization, which develops various software packages. The most important element of this license is that instead of protecting a particular person or company, it protects the software code that creates the application.

Determining Which Ports to Block

When determining which ports to block on your server, you must first determine which services you require. In most cases, block all ports that are not exclusively required by these services. This is tricky, because you can easily block yourself from services you need, especially services that use ephemeral ports. If your server is an exclusive e-mail server running SMTP and IMAP, you can block all TCP ports except ports 25 and 143, respectively. If your server is an exclusive HTTP server, you can block all ports except TCP port 80.

Learn How to Set Preferences For TkAntivir

SECURITY ALERT!

Although Tripwire has a "file integrity mode," Tripwire is not really an integrity checker in the classic sense. It does not, for example, test the file's stability or inode number or any other aspect in regards to file storage. Tripwire simply compares a file's new signature with that taken when the database was created. Other tools may be used to check the integrity of a file's permissions and ownership information.

Learn the Flags Used in TCP Connections

Flag	Description
SYN	Synchronize sequence numbers. Used for connection establishment.
FIN	The sender is finished with the connection. Used for connection termination.
RST	Reset the connection.
PSH	Push the data.
ACK	Acknowledgment
URG	Urgent

Answer Your Questions about Kerberos

Q: I wish to remove a principal from the keytab of one of my Kerberos clients. How do I do this?

A: Enter kadmin as an administrative user on the Kerberos client (not the KDC) and use the **ketremove** option. For example, if you wanted to remove the principal for the user named *james*, you would do the following:

```
terminal$/usr/
 kerberos/sbin/kadmin
kadmin: ktremove
 -p james
kadmin: quit
terminal$
```

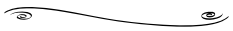
Secure E-Commerce Transactions

If hackers were alerted to an unsecure server, they could capture packets going in and out of the server to gain the data they sought. For example, if an e-commerce server does not use any type of network encryption for transactions, there is a great deal of data to be gained by a hacker. Unfortunately, many small companies or entrepreneurs set up their own Web servers, unaware of potential security problems, and set up simple scripts to process payment forms.

Secure Tunneling with Virtual Private Networks (VPNs)

VPNs provide a private data network over public telecommunication infrastructures, such as the Internet, by providing authentication and encryption through a data "tunnel" between devices. All data transmitted between the devices through the tunnel is secure, regardless of what programs the devices are running.

Understand Essential Linux Firewall Functions



- IP address conservation and traffic forwarding
- Network differentiation
- Protection against denial-of-service, scanning, and sniffing attacks
- IP and port
- Content filtering
- Packet redirection
- Enhanced authentication and encryption
- Supplemented logging

Configure Squid with the /etc/squid/squid.conf file

See How to Use the Firelogd Program

Firelogd (Firewall Log Daemon) is a relatively simple program that can either be run as an application or (you might have guessed) as a daemon. It does two things:

- It reads the kernel log entries and passes them into a "first in, first out" (FIFO) pipe, which Firelogd can then process.
- Once its buffer is full, it e-mails a report of suspicious traffic to an account of your choosing. You can have it mailed to a local account, or to a remote system of your choice.

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

Chapter 1

Introduction to Open Source Security

Solutions in this chapter:

- Using the GNU General Public License
- Soft Skills: Coping with Open Source Quirks
- Should I Use an RPM or Tarballs?
- Obtaining Open Source Software
- A Brief Encryption Review
- Public Key and Trust Relationships
- Auditing Procedures

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

In spite of the ups and downs of the dot-com industry, open source software has become a viable alternative to commercial companies such as Microsoft, Sun, and IBM. Although open source software has its quirks and its problems, the open source movement has made its niche in the networking market. As a networking professional, it is in your best interest to understand some of the more important security applications and services that are available.

This book is designed to provide experienced systems administrators with open source security tools. Although we have made every effort to include as many people and as many skill sets as possible, this book assumes a fundamental knowledge of Linux. This book focuses on open source Linux applications, daemons, and system fixes. In the book's first chapters, you will learn how to lock down your network. Chapter 2 discusses ways to secure and monitor the operating system, and ways to scan local and remote networks for weaknesses. You will receive detailed information on how to ensure that your system's services and the root account are as secure as possible.

In Chapter 3, you will learn how to deploy antivirus and scanning programs for your local system. By using these scanning programs, you will be able to mitigate risk and learn more about the nature of services on your network. Scanners such as nmap and nessus will help you learn about the open ports on your network, and how these open ports might pose a threat to your system. Chapter 3 gives you detailed information about practical ways to implement intrusion detection on your local system and on your network. Using applications such as Tripwire, Portsentry, and Snort, you will be able to precisely identify system anomalies and detect inappropriate logins. Chapter 5 shows how you can use open source tools such as tcpdump, Ethereal, EtherApe, and Ntop to inspect and gauge traffic on the network.

The second part of the book focuses on ways to enhance authentication using open source software. In Chapter 6, you will learn about One Time Passwords (OTP) and Kerberos as ways to ensure that malicious users won't be able to obtain your passwords as they cross the network. Chapter 7 discusses ways to use Secure Shell (SSH) and Secure Sockets Layer (SSL), which are ways to enable on-the-fly encryption to protect data. In Chapter 8, you will learn about how to enable IPSec on a Linux system so that you can implement a virtual private network (VPN). As you learn more about the primary VPN product called Free Secure Wide Area Network (FreeS/WAN), you will see how it is possible to protect network traffic as it passes through your own network, and over the Internet.

The final part of the book focuses on ways to create an effective network perimeter. Chapter 9, shows how to install and configure Ipchains and Iptables on a Linux system. Kernels earlier than 2.3 can use Ipchains, whereas kernel versions 2.3 and later use Iptables. Regardless of the way you do it, you will learn to filter traffic with these two packet filtering tools.

In Chapter 10, you will learn how a proxy server can further enhance your control over your network perimeter. Specifically, you will use the Squid proxy server to control client access to the Internet. You will also learn how to configure Linux clients to access the proxy server. Finally, Chapter 11, shows how to troubleshoot and counteract problems with your network perimeter. You will learn how to maintain, test, and log the firewall so that you have a functional barrier between you and the outside world.

It is our intention to create a book that gives you practical information and advice about the most common open source security tools.

The Tools Used in This Book

This book was written using version 7.0 of the Red Hat Linux operating system. Although it may not be the "best" Linux distribution (there are at least 100 versions in the world), it is the most popular. We have tried to ensure that the skills and tools you obtain in this book will be portable to other Linux versions, and even other open source operating systems such as FreeBSD (www.freebsd.org). However, each Linux flavor has its own quirks, and you may find it necessary to deviate from some of the instructions in this book.

Using the GNU General Public License

The GNU General Public License (GPL) is the basis of the open source movement. This license is provided by the Gnu is Not Unix (GNU) organization, which develops various software packages. Begun in 1984 by Richard Stallman, GNU has worked to create a license designed to ensure that the open source movement continues to thrive. You can learn more about GNU at the www.gnu.org Web site, shown in Figure 1.1.

The most important element of this license is that instead of protecting a particular person or company, it protects the software code that creates the application. Traditionally, copyrights have enabled individuals to lay claim to a particular piece of software and then sell it for profit. In addition, the copyright enables that individual to then take action against anyone else who uses that code to create

similar functionality. For better or for worse, Richard Stallman, Eric Raymond, and others helped found and popularize the concept of an open software license called the Gnu General Public License (often referred to as the *GPL*). You can read the GPL at www.gnu.org/copyleft/gpl.html.

Figure 1.1 The GNU Web Site

This license is part of the "copyleft" movement, which considers itself an alternative to traditional copyright laws. The GPL essentially allows anyone who develops code to ensure that the code remains open, meaning that GPL-licensed code can be taken and improved upon by anyone, as long as the improved code is given to the original writer and the software writing community. Consequently, a piece of code protected by the GPL will, by law, always remain accessible by anyone who wants to read or modify it. Without the GPL license, another person can take the code that you invent, and make it closed and proprietary.

The GNU GPL is not the only free software license in existence. Figure 1.2 shows the GNU page dedicated to understanding additional licenses. If you wish, you can read about additional licenses that are similar to the GPL at www.gnu.org/philosophy/license-list.html.

For more information about the open source movement, one of the more revealing books is Erik Raymond's *The Cathedral and the Bazaar* (O'Reilly &

Associates, 2001). Although somewhat overly enthusiastic, it is a very helpful book in understanding the mindset of many open source code writers.

Figure 1.2 Viewing GNU's Licenses Comment Section

Fee-Based GPL Software

Contrary to what you might think, open source code protected by the GPL is not necessarily free. Under the terms of the GPL, any person or corporation can take GPL software, modify it, and then package it for sale. However, this person or corporation must make this software freely available for anyone to read or modify.

Can I Use GPL Software in My Company?

The GNU GPL does not ask companies to supply licensing agreements or otherwise register the programs. However, other licenses, which you can read at GNU's comparative forum, may invoke restrictions that you may have to consider as you implement the software. The software covered in this book is, in one way or another, open software, which means it can be used by any organization.