Linux Server Security
**Synopsis**

Linux consistently appears high up in the list of popular Internet servers, whether it’s for the Web, anonymous FTP, or general services such as DNS and delivering mail. But security is the foremost concern of anyone providing such a service. Any server experiences casual probe attempts dozens of time a day, and serious break-in attempts with some frequency as well. This highly regarded book, originally titled Building Secure Servers with Linux, combines practical advice with a firm knowledge of the technical tools needed to ensure security. The book focuses on the most common use of Linux—as a hub offering services to an organization or the Internet—and shows readers how to harden their hosts against attacks. An all-inclusive resource for Linux users who wish to harden their systems, Linux Server Security covers general security such as intrusion detection and firewalling a hub, as well as key services such as DNS, the Apache Web server, mail, and secure shell.

Author Michael D. Bauer, a security consultant, network architect, and lead author of the popular Paranoid Penguin column in the Linux Journal, carefully outlines the security risks, defines precautions that can minimize those risks, and offers recipes for robust security. He is joined on several chapters by administrator and developer Bill Lubanovic. A number of new security topics have been added for this edition, including: Database security, with a focus on MySQL, Using OpenLDAP for authentication, An introduction to email encryption, The Cyrus IMAP service, a popular mail delivery agent, The vsftpd FTP server.

Geared toward Linux users with little security expertise, the author explains security concepts and techniques in clear language, beginning with the fundamentals. Linux Server Security with Linux provides a unique balance of “big picture” principles that transcend specific software packages and version numbers, and very clear procedures on securing some of those software packages on several popular distributions. With this book in hand, you’ll have both the expertise and the tools to comprehensively secure your Linux system.

**Book Information**

Paperback: 544 pages  
Publisher: O’Reilly Media; 2 edition (January 28, 2005)  
Language: English  
ISBN-10: 0596006705  
Product Dimensions: 7 x 1.1 x 9.2 inches  
Shipping Weight: 1.6 pounds (View shipping rates and policies)

Average Customer Review: 3.8 out of 5 stars Â – See all reviews Â (10 customer reviews)
Linux Server Security, Second Edition
By Michael D. Bauer
Second Edition January 2005
544 pages, $44.95 US

This book goes along with the moving trend of the normal computer user, securing your data. Servers generally are targeted more often than the average home PC because most are made to be accessible from the outside world. This is where securing that server comes into play. This book covers the tools and techniques to securing your Bastion host.

First I’d like to start out and explain what Bastion host means as according this book so you can understand what this book covers more specifically. Bastion Host is defined as "A system that runs publicly accessible services but is usually not itself a firewall. Bastion hosts are what we put on DMZ (although they can be put anywhere). The term implies that a certain amount of system hardening has been done, but sadly, this is not always the case." After you understand what a Bastion host is defined as, you should understand that this book mainly covers these server daemons and the systems that run them. But some of the information applies to a Linux desktop system such as a per host iptables firewall, using secure shell, keeping up with your logs, and intrusion detection. Most of these things the average user doesn’t care much about but sometimes being paranoid comes in handy.

Someone who would most likely use this book more than the average desktop user would probably be a system administrator. Securing web, database, ftp, dns, and email servers is what majority of this book contains. Along with covering these server systems, there are guides to securing the Linux system that runs these daemons along with designing the networks around these types of hosts.

Customer Reviews

Download to continue reading...

Red Hat Enterprise Linux (RHEL) 7 Server Installation and Administration: Training Manual: Covering CentOS-7 Server, Cloud computing, Bind9 DNS Server and Fedora 23 Server
Red Hat Enterprise Linux (RHEL) 6 Server Installation & Administration: Training Manual: Covering CentOS-6, OpenSUSE 11.3 Server, Mandriva Enterprise Server, and Fedora 14 Server

Dmca