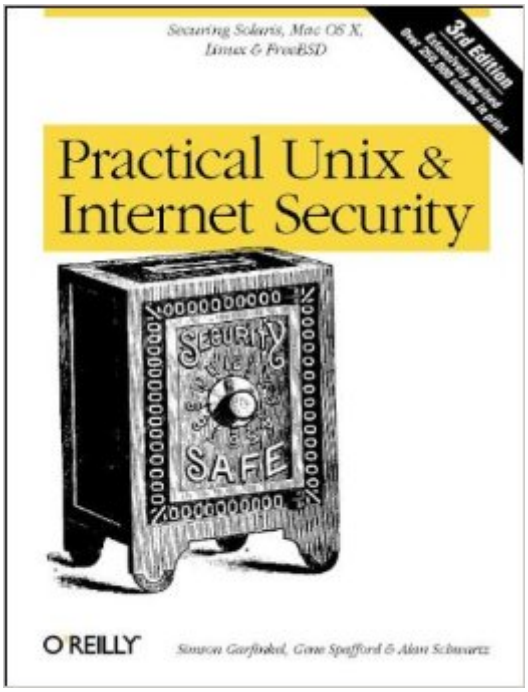
Practical Unix & Internet Security, 3rd Edition



Synopsis

When Practical Unix Security was first published more than a decade ago, it became an instant classic. Crammed with information about host security, it saved many a Unix system administrator from disaster. The second edition added much-needed Internet security coverage and doubled the size of the original volume. The third edition is a comprehensive update of this very popular book - a companion for the Unix/Linux system administrator who needs to secure his or her organization's system, networks, and web presence in an increasingly hostile world.Focusing on the four most popular Unix variants today--Solaris, Mac OS X, Linux, and FreeBSD--this book contains new information on PAM (Pluggable Authentication Modules), LDAP, SMB/Samba, anti-theft technologies, embedded systems, wireless and laptop issues, forensics, intrusion detection, chroot jails, telephone scanners and firewalls, virtual and cryptographic filesystems, WebNFS, kernel security levels, outsourcing, legal issues, new Internet protocols and cryptographic algorithms, and much more.Practical Unix & Internet Security consists of six parts:Computer security basics: introduction to security problems and solutions, Unix history and lineage, and the importance of security policies as a basic element of system security.Security building blocks: fundamentals of Unix passwords, users, groups, the Unix filesystem, cryptography, physical security, and personnel security.Network security: a detailed look at modem and dialup security, TCP/IP, securing individual network services, Sun's RPC, various host and network authentication systems (e.g., NIS, NIS+, and Kerberos), NFS and other filesystems, and the importance of secure programming.Secure operations: keeping up to date in today's changing security world, backups, defending against attacks, performing integrity management, and auditing.Handling security incidents: discovering a break-in, dealing with programmed threats and denial of service attacks, and legal aspects of computer security.Appendixes: a comprehensive security checklist and a detailed bibliography of paper and electronic references for further reading and research.Packed with 1000 pages of helpful text, scripts, checklists, tips, and warnings, this third edition remains the definitive reference for Unix administrators and anyone who cares about protecting their systems and data from today's threats.

Book Information

Paperback: 988 pages
Publisher: O'Reilly Media; 3 edition (March 3, 2003)
Language: English
ISBN-10: 0596003234
ISBN-13: 978-0596003234

Product Dimensions: 7 x 2.1 x 9.2 inches

Shipping Weight: 3 pounds (View shipping rates and policies)

Average Customer Review: 4.3 out of 5 starsÂ Â See all reviewsÂ (43 customer reviews)

Best Sellers Rank: #573,404 in Books (See Top 100 in Books) #12 inÂ Books > Computers & Technology > Operating Systems > Unix > Administration #12 inÂ Books > Computers & Technology > Programming > APIs & Operating Environments > Device Drivers #135 inÂ Books > Computers & Technology > Certification > CompTIA

Customer Reviews

Somewhat outdated -- two years old in a very dynamic field, Rootkit is not even mentioned, Bugtraq mentioned only in supplement, etc. Far from being practical and can be used only as an introductory text in Unix security. Not recommended for Internet security (superficial and incomplete). Good style -- Simson Garfinkel of The UNIX-Haters Handbook fame is a really talented journalist (but now only a journalist, see his interview with .com). The main problem with the book is that instead of relying on tools as any Unix author should, the authors use a cookbook/reference approach giving recipes about improving security. References to important RFCs, FAQ and CERT advisories are absent. For example RFC1244 (now superseded by RTC2196) is not mentioned in index(and probably in the text as well) although Ch.2 and Ch.24 mirror its content. No attempts were made to explain what tools can be used for checking/fixing particular class of problems or to present a bigger picture in which the flaw exists. Typesetting is very primitive. Although one of the authors is a (former) programmer judging by just the book content it is difficult to believe that he is able to spell PERL :-). The book is not updated enough to compete with newer books on Internet Security. For corporate users possible alternatives are combinations of one book on Unix security (for example, Unix System Security by David A. Curry) and one book on Internet security (for example Actually Useful Internet Security Techniques by Larry J. Hughes). The last is recommended as an alternative for readers who cannot afford two books. Often books written by a specialist in particular areas can be a better deal than books from security folks. For example TCP/IP Network Administration by Craig Hunt contains a lot more information about how properly configure TCP/IP than this book and in Ch.12 has a very decent overview of security in just 40 pages.

As a Linux administrator, I ordered this book hoping to find out how hackers typically gain access to systems and neat little tricks for locking down my system, as well as detecting and dealing with intruders. While Practical Unix & Internet Security did cover these topics, it covered little I didn’t

already know.Significant time is spent explaining how unix-based systems work. The book covers things such as file systems, partition structure, file ownership/permissions, users and groups, inodes, ssh, backups, etc. Each command, utility, procedure or feature is detailed over several pages followed by an explanation of what you should be doing with said topic.There are also a few real-world examples here and there; stories most of us have heard before, like the admin who had . in his path.Unlike many computer books, this one is well written and an easy read, and it's certainly a lot more friendly than some unix geek's advice which consists of RTFM.I think this book would be great for someone who has a very basic understanding of unix-based systems but has never administrated one before, but for those of us who've already had some experience running unix there's probably not anything new here for you.

This books is a very thorough hands-on guide to the subject of security for unix computers connected to the Internet.It starts with basic subjects, such as passwords, backups, security auditing & logging, and physical security, and then continues with networking subjects, such as modems, TCP/IP, NFS, kerberos, firewalls, proxies, etc. important issues and terms are interwined - such as what is the rainbow series and legal issues.The subject of computer & Internet security is changing quickly, and as other reviewers have written a book written a couple of years ago (I have the 1996 edition) is no longer up to date.But I think it's a minor issue.First, because one must still learn and protect against older attacks - an intruder will not shy away from trying to use an old security hole just because it's two months old. Hacks are not cheese, and cant be thrown out after two weeks.Second, a sysadmin should get the basic information, terms, ways of thought, etc - and this book will teach this well - and then continuously look for new information and information sources.This includes finding out about bugtraq, ntbugtraq, phrack, and any other new mailing lists and web sites regularily.So I highly recommend this book to anyone who deals with the subject of unix & internet security.

The second edition of this book was my security vade mecum for the last 8 years. For what I can foresee, this third edition, will play the same role for (at least) the next three years.When you are required as an security expert, several tasks are usually to be faced:New scenarios to analyze?, checklists to recommend?, good firewall architectures to suggest?, logs to watch? (and so on). Don't worry, with the only help of this Garfinkel, Spafford and Schwartz 'little giant' book, you are done.Excellent book. A Must for security people.

The best beginners guide to UNIX security and computer security in general I have ever read. In fact the only technical book I have read and enjoyed! This book explains first principles in computer security in an understandable way. This is particularly useful for computer auditors, who may not be technically competent in UNIX. I used this book to develop security audit programs for backup and recovery, incident management, basic UNIX security review and risk management. Consequently I was haled as a hero and a guru by management! New computer auditors should buy this now!

Practical Unix & Internet Security, 3rd Edition Unix, Solaris and Linux: A Practical Security Cookbook: Securing Unix Operating System Without Third-Party Applications Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Python para administracion de sistemas Unix y Linux/ Pythons for Management of Unix and Linux Sistems (Spanish Edition) Unix Desktop Guide to the Korn Shell (Unix Desktop Guides) Conducting the UNIX Job Interview: IT Manager Guide with UNIX Interview Questions (IT Job Interview series) UNIX from Soup to Nuts: A Guide and Reference for UNIX Users and Administrators Unix System V/386 Release 3.2: System Administrator's Guide (AT&T UNIX system V/386 library) Teach Yourself the Unix C Shell in 14 Days (Unix Library) Advanced Unix Shell Scripting: How to Reduce Your Labor and Increase Your Effectiveness Through Mastery of Unix Shell Scripting and Awk Programming Unix Shell Programming Tools with CDROM (Unix Tools) UNIX AWK and SED Programmer's Interactive Workbook (UNIX Interactive Workbook) Unix Commands by Example: A Desktop Reference for Unixware, Solairs and Sco Unixware, Solaris and Sco Unix The Waite Group's Unix Communications and the Internet UNIX Administration: A Comprehensive Sourcebook for Effective Systems & Network Management (Internet and Communications) Unix/Linux Survival Guide (Networking & Security) UNIX(R) System Security: A Guide for Users and System Administrators Security Analysis: Sixth Edition, Foreword by Warren Buffett (Security Analysis Prior Editions) By Graham Glass - UNIX for Programmers and Users: 3rd (third) Edition UNIX for Programmers and Users by Glass, Graham, Ables, King [Prentice Hall, 2003] (Paperback) 3rd Edition [Paperback]