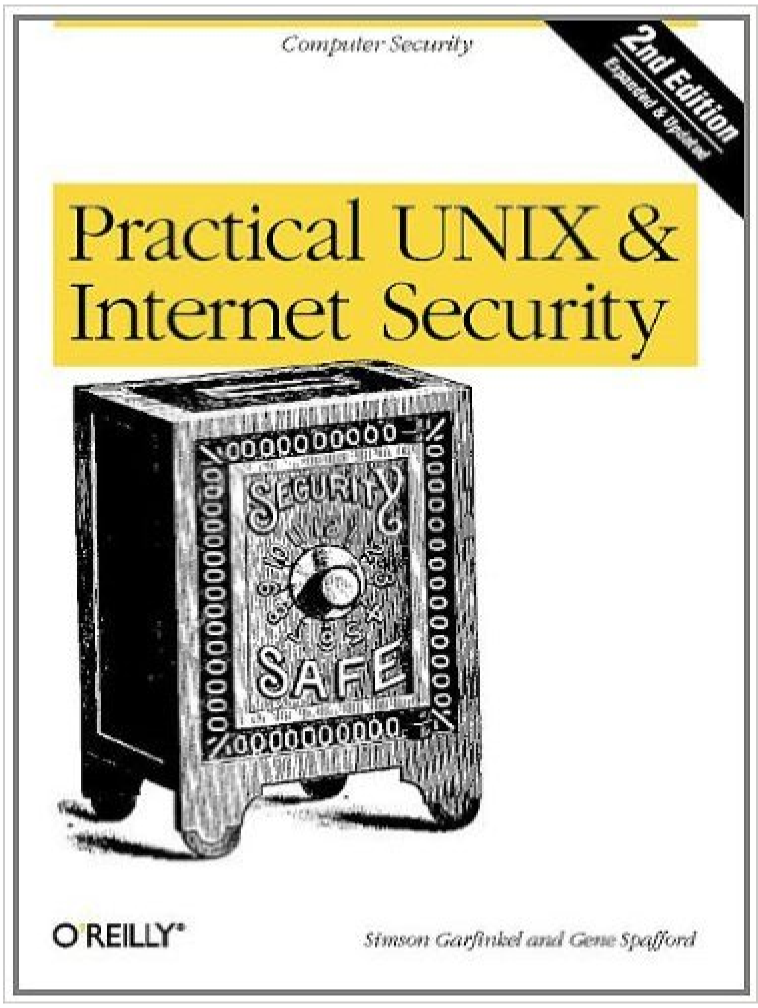
Practical UNIX And Internet Security (Computer Security)



Synopsis

When Practical UNIX Security was first published in 1991, it became an instant classic. Crammed with information about host security, it saved many a UNIX system administrator and user from disaster.This second edition is a complete rewrite of the original book. It’s packed with twice the pages and offers even more practical information for UNIX users and administrators. It covers features of many types of UNIX systems, including SunOS, Solaris, BSDI, AIX, HP-UX, Digital UNIX, Linux, and others. The first edition was practical, entertaining, and full of useful scripts, tips, and warnings. This edition is all those things -- and more.If you are a UNIX system administrator or user in this security-conscious age, you need this book. It’s a practical guide that spells out, in readable and entertaining language, the threats, the system vulnerabilities, and the countermeasures you can adopt to protect your UNIX system, network, and Internet connection. It’s complete -- covering both host and network security -- and doesn’t require that you be a programmer or a UNIX guru to use it.Practical UNIX & Internet Security describes the issues, approaches, and methods for implementing security measures. It covers UNIX basics, the details of security, the ways that intruders can get into your system, and the ways you can detect them, clean up after them, and even prosecute them if they do get in. Filled with practical scripts, tricks, and warnings,Practical UNIX & Internet Security tells you everything you need to know to make your UNIX system as secure as it possible can be.Contents include:Part I: Computer Security Basics. Introduction and security policies.Part II: User Responsibilities. Users and their passwords, groups, the superuser, the UNIX filesystem, and cryptography.Part III: System Administrator Responsibilities. Backups, defending accounts, integrity checking, log files, programmed threats, physical security, and personnel security.Part IV: Network and Internet Security: telephone security, UUCP, TCP/IP networks, TCP/IP services, WWW, RPC, NIS, NIS+, Kerberos, and NFS.Part V: Advanced Topics: firewalls, wrappers, proxies, and secure programming.Part VI: Handling Security Incidents: discovering a breakin, U.S. law, and trust.VII: Appendixes. UNIX system security checklist, important files, UNIX processes, paper and electronic sources, security organizations, and table of IP services.

Book Information

Series: Computer Security

Paperback: 1004 pages

Publisher: O’Reilly Media; 2 edition (April 11, 1996)

Language: English

ISBN-10: 1565921488

ISBN-13: 978-1565921481

Product Dimensions: 7 x 2.1 x 9.2 inches

Shipping Weight: 2.8 pounds

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

Best Sellers Rank: #4,171,224 in Books (See Top 100 in Books)   #74 inÂ Books > Computers & Technology > Programming > APIs & Operating Environments > Device Drivers   #932 inÂ Books > Computers & Technology > Certification > CompTIA   #1119 inÂ Books > Computers & Technology > Operating Systems > Unix

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!

Download to continue reading...

Ideas & Internet Marketing Tips fo Book 1) Security, Rights, & Liabilities in E-Commerce (Artech House Computer Security Series) Beyond Powerful Radio: A Communicator's Guide to the Internet Age_News, Talk, Information & Personality for Broadcasting, Podcasting, Internet, Radio