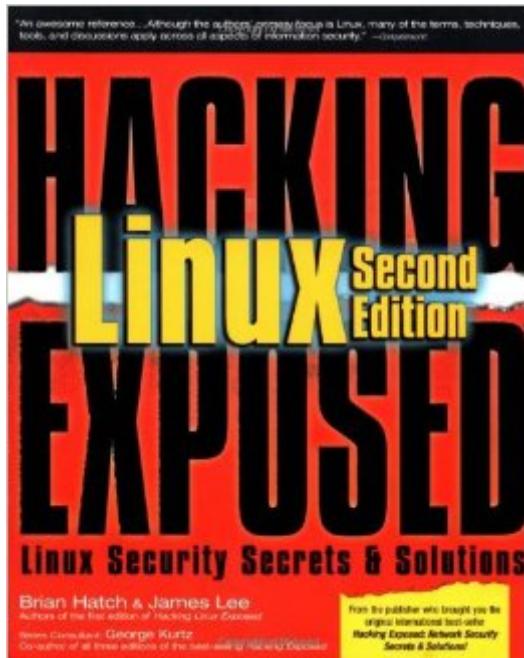


The book was found

Hacking Linux Exposed, Second Edition



Synopsis

Tighten holes and maintain security on your Linux system! From the publisher of the international best-seller, Hacking Exposed: Network Security Secrets & Solutions, comes this must-have security handbook for anyone running Linux. This up-to-date edition shows you how to think like a Linux hacker in order to beat the Linux hacker. You'll get detailed information on Linux-specific hacks, both internal and external, and how to stop them.

Book Information

Series: Hacking Exposed

Paperback: 712 pages

Publisher: McGraw-Hill Osborne Media; 2 edition (December 4, 2002)

Language: English

ISBN-10: 0072225645

ISBN-13: 978-0072225648

Product Dimensions: 7.3 x 1.5 x 9 inches

Shipping Weight: 3 pounds

Average Customer Review: 4.9 out of 5 starsÂ [See all reviewsÂ \(41 customer reviews\)](#)

Best Sellers Rank: #1,329,751 in Books (See Top 100 in Books) #285 inÂ Books > Computers & Technology > Operating Systems > Linux > Programming #313 inÂ Books > Computers & Technology > Operating Systems > Linux > Networking & System Administration #453 inÂ Books > Computers & Technology > Operating Systems > Unix

Customer Reviews

I am a senior engineer for network security operations. I read "Hacking Linux Exposed" (HLE) to learn how adversaries compromise Linux hosts. HLE impressed me at every level. I highly recommend system administrators and security personnel read and heed this book's recommendations. The "Hacking Exposed" series is known for its unique example-driven style. Rather than telling the reader about a technique or problem, the authors demonstrate the issue using command-line examples. I find myself reading with book and laptop at hand, ready to duplicate the authors' sample commands. This process reinforces the authors' message, while the reader learns if a specific problem applies to his situation. Furthermore, by showing exactly how to execute certain commands, the authors impart bits of wisdom and trickery not found elsewhere. For example, chapter 11 describes attacks and defenses for FTP servers. To explain active and passive FTP sessions, the authors demonstrate running an FTP client with the -d switch to illustrate raw

instructions sent by the client over the FTP command channel. I had never seen this switch in use, but as an intrusion detector I constantly see raw FTP instructions like those revealed by the -d switch. These and other tidbits, like using the chattr -i command or setting the "sticky bit", make HLE exceptional. Beyond these benefits, readers will enjoy clear, thorough explanations of Linux security issues. HLE gives first-rate descriptions of ssh and web man-in-the-middle attacks, race conditions, and FTP data hijacking. HLE also provides great illustrated examples of FTP bounce attacks, giving intrusion detectors the minutiae we need to recognize these techniques.

I wasn't a fan of Hacking Exposed, largely because its Unix section was a mere 50 pages of superficial, outdated, and obvious fluff. Hacking Linux Exposed makes up for that lack by digging into Unix in much more depth. Though it is modeled after the attack/countermeasure style of the original HE, this book includes a whole chapter of security measures at the beginning that you can implement instantly to get your machine locked down before getting into the nitty-gritty detail about other things in the hacker's arsenal. I was particularly enthralled with chapter 10, which talks about what the hacker will do after they have gained root access, from simple things like adding accounts to complicated issues like kernel modules, complete with source code. Chapter 7 includes some really wonderful examples of how the hacker can abuse networking protocols themselves, something I haven't seen covered in such depth before. The book is logically organized. The first part covers the way the hackers find and probe your machine. The second talks about getting in from the outside, be it network or physical. The third part talks about gaining additional privileges, and the last part of the book is dedicated to mail, ftp, web, and firewalls. The appendices are actually useful. They seem to have dropped the small 1-page case studies from the original book and replaced them with longer hacker-eye-views of real attacks which are an interesting read, and really tie the book together. This book is Linux specific in its countermeasures, but I'd recommend this to any unix user. They do a good job of discussing differences between Linux variants as well, they don't just assume everyone has a RedHat box on their desk. Very refreshing. This book is great for both the theory and practical uses.

[Download to continue reading...](#)

Hacking: The Ultimate Beginners Guide (Computer Hacking, Hacking and Penetration, Hacking for dummies, Basic security Coding and Hacking) (Hacking and Coding Book 1) Hacking: Ultimate Hacking for Beginners, How to Hack (Hacking, How to Hack, Hacking for Dummies, Computer Hacking) Hacking: Wireless Hacking, How to Hack Wireless Networks, A Step-by-Step Guide for Beginners (How to Hack, Wireless Hacking, Penetration Testing, Social ... Security, Computer

Hacking, Kali Linux) LINUX: Linux Command Line, Cover all essential Linux commands. A complete introduction to Linux Operating System, Linux Kernel, For Beginners, Learn Linux in easy steps, Fast! A Beginner's Guide Hacking University: Freshman Edition Essential Beginner's Guide on How to Become an Amateur Hacker (Hacking, How to Hack, Hacking for Beginners, Computer ... (Hacking Freedom and Data Driven Book 1) Hacking University: Sophomore Edition. Essential Guide to Take Your Hacking Skills to the Next Level. Hacking Mobile Devices, Tablets, Game Consoles, and ... (Hacking Freedom and Data Driven Book 2) Hacking: How to Hack Computers, Basic Security and Penetration Testing (Hacking, How to Hack, Hacking for Dummies, Computer Hacking, penetration testing, basic security, arduino, python) HACKING: Learn Hacking FAST! Ultimate Course Book For Beginners (computer hacking, programming languages, hacking for dummies) Hacking: The Ultimate Beginners Guide (Hacking, How to Hack, Hacking for Dummies, Computer Hacking, Basic Security) Hacking: Beginner's Guide to Computer Hacking, Basic Security, Penetration Testing (Hacking, How to Hack, Penetration Testing, Basic security, Computer Hacking) Wireless Hacking: How To Hack Wireless Network (How to Hack, Wireless Hacking, Penetration Testing, Social ... Security, Computer Hacking, Kali Linux) Linux: Linux Guide for Beginners: Command Line, System and Operation (Linux Guide, Linux System, Beginners Operation Guide, Learn Linux Step-by-Step) Hacking Linux Exposed, Second Edition Hacking Exposed Linux, 3rd Edition HACKING: Beginner's Crash Course - Essential Guide to Practical: Computer Hacking, Hacking for Beginners, & Penetration Testing (Computer Systems, Computer Programming, Computer Science Book 1) Hacking: The Beginners Guide to Master The Art of Hacking In No Time - Become a Hacking GENIUS Hacking: How to Computer Hack: An Ultimate Beginner's Guide to Hacking (Programming, Penetration Testing, Network Security) (Cyber Hacking with Virus, Malware and Trojan Testing) C++: C++ and Hacking for dummies. A smart way to learn C plus plus and beginners guide to computer hacking (C++ programming, C++ for Beginners, hacking, ... language, coding, web developing Book 2) Linux: Linux Mastery. The Ultimate Linux Operating System and Command Line Mastery (Operating System, Linux) Hacking Exposed Malware & Rootkits: Security Secrets and Solutions, Second Edition

[Dmca](#)