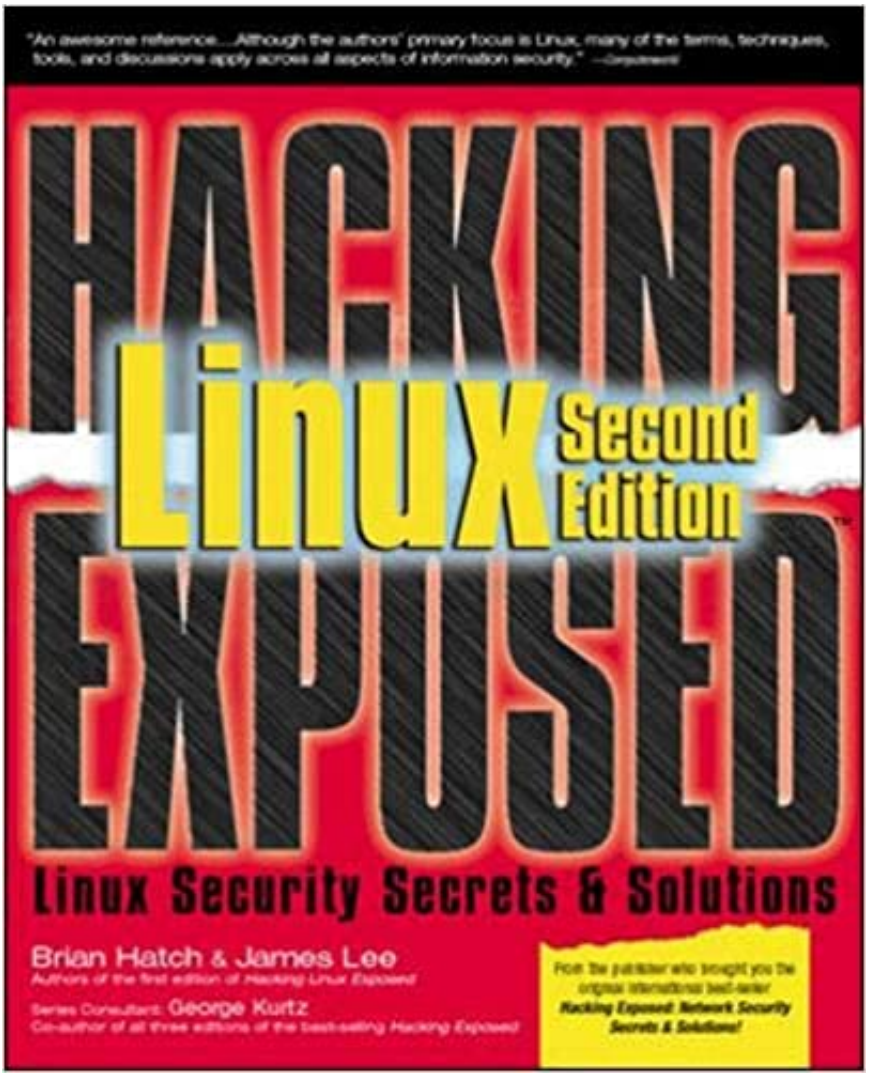
Hacking Linux Exposed, Second Edition



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.

Sort review

"Throw up a Linux box," comes the chorus whenever there's a need to provide some network service or other without impinging upon the boss's martini budget. Fair enough, but by doing so are you opening security holes you don't know how to find or fix? The newest edition of Hacking Linux Exposed helps you answer that question and solve many of the security problems you find. To a certain extent this book is a recipe collection in that it describes weaknesses in Linux (calling attention to specific distributions where appropriate). The authors stop short of explicitly showing you how to wage most kinds of attacks, a reasonable thing to do from an ethical point of view even though the instructions can be found easily on the Internet. Rather than do that, they give step-by-step instructions on how to defend against the attacks they catalog. The point is not, "Here's precisely how to bring down a server by means of an ACK storm," but rather, "Here's how to defend against such problems." They do demonstrate plenty of weaknesses, though, as in their coverage of the conversation that goes back and forth between an FTP server and its client.This book covers pretty much everything you'd want to do with a Linux machine as a network server. Read it and see some of the weaknesses in your system--and do something about them before someone else does. --David WallTopics covered: Security best practices, approached from the perspective of what can go wrong and what can be done about the problems. Specific coverage goes to all major services, including user management, FTP, HTTP, and firewalling.From the Back Cover"Years of collective hands-on expertise for those who want to actually understand the Linux threats and countermeasures. Excellent!" --Dave Wreski, CEO, Guardian Digital and co-author of Linux Security HOTWOSecure your Linux network by thinking like an attackerEvolving Web technology and new software releases make online security more challenging than ever. The number of hackers--both sophisticated crackers and script-kiddies--is growing constantly, and it's just a matter of time before your network becomes a target. Hacking Linux Exposed, Second Edition shows you, step-by-step, how to proactively defend against the latest Linux-specific attacks by getting inside the mind of today's most devious hackers. You'll learn how intruders gather information, specify targets, exploit weak spots, and gain control--usually while remaining undetected. Read case studies about both common and little-known break-ins, tips on how and why they occurred, and detailed countermeasures against these attacks. If you're a Linux professional who's serious about security, this is the one book you can't

afford to be without.What you'll learn:The proven Hacking Exposed methodology to locate and fix vulnerable points in networks and Linux softwareDetails on security features of all Linux distributions--including Red Hat, Debian, SuSE, and SlackwareHow to successfully use vulnerability scanning tools, intrusion detections systems, honeypots, and log analysis softwareBest practices for using whois databases, ping sweeps, DNS zone transfers, and port scansCommon mail server bugs, tips for email encryption, and spam preventionLatest attack methods involving Trojaned programs, back doors, kernel hacks, password cracks, and session hijackingWays to protect against Denial of Service and wireless network attacksMethods for preventing local users from getting root privilegesRules for using TCP wrappers and firewall strategies with ipchains and iptablesValuable checklists and tips on hardening your system based on the authors' real-world experienceAbout the AuthorBrian Hatch is a UNIX/Linux security consultant, administrator, and expert hacker with Onsight, Inc. He has taught various courses at Northwestern University and is the co-maintainer of Stunnel, a widely used secure SSL wrapper. He is the lead author of the first edition of Hacking Exposed Linux.James Lee is a Perl hacker, Linux administrator, security consultant, and open source advocate. James is the founder and CEO of Onsight Inc., a consulting firm specializing in Perl training and web development. James is also a co-author of the first edition of Hacking Exposed Linux.George Kurtz, co-author of all three editions of the international best-seller, Hacking Exposed, and co-author of Hacking Exposed Linux is the CEO of Foundstone, Inc., a premier security consulting and training company.Read more

What people say about this book

Doug M, “Refreshingly honest, thoroughly enlightening. Given the complexity of Linux systems, and the years spent hardening such systems against would-be intruders, it is amazing how a simple, clever idea can still translate into a full-blown security exploit.I really enjoyed the format of the book. The authors don't waste time on security theories, or explaining what Linux is. They know the reader is already familiar with these, and wants to know, in concrete terms, how a hacker sees your server, and will systematically breach its security until they get root access. The authors waste no time in revealing the tools of the trade, and the security-conscious would do well to read this book from cover to cover. It is not enough to just apply patches, and turn off unnecessary services (and surprisingly few admins even do this right). One must fully understand the mindset of the hacker, and see the server from the outside.I truly believe that no other book right now can deliver such honesty and such useful information on Linux security. If you hope to secure your servers or go into the security field, definitely read this book. You will not be sorry. :)”

Gavin Rollins, “Can't put it down!!. The book pulls you into a hackers/crackers mind! no boring bla-bla text that puts you to sleep in 3 minutes! the only reason I gave it 4 stars is that it didn't come with a CD! Most of the books I've read came with the programs they discussed in the book, This was my only let down. I've contacted the authors about some questions and I received a fast and curtious reply. Hats off to you Gents, and I must thank Brian for his reply,about to much security, your one of the reasons I've switched from windows to linux. Try and contact Bill if ya got a question about windows!”

Comms Guy, “Five Stars. Good info.”

Ebook Library Reader, “Buy two of these. 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 priveleges, and the last part of the book is dedicated to mail, ftp, web, and firewalls. The appendicies 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 it's 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. I could spend weeks implementing all the suggestions they have, but they seem to have thought of this because their risk ratings let you know where you should concentrate as you secure your systems.Like Hacking Exposed, this book also has a website, (...) but it seems more up-to-date -- for example when the ptrace bug in older kernels came out, they posted a kernel module you could compile to protect your system until you could upgrade -- and includes all the source code contained in the book.I bought two of these, one for home and one for the office, and I suggest you do the same."

Trin, "Worth it many times over!. Hacking Linux comes in six parts, each of which is worth the price of the book in whole. Part one: security overview covers all the basics like file permissions, setuserid problems, buffer overflows/format string attacks, tools to use before you go online, and mapping tools like nmap. Part two comes in from more of the hacker angle with social engineering and trojans, attacks from the console, and then concludes with two excellent chapters about netowrk attacks and TCP/IP vulnerabilities.All the stuff to this point assumes the hacker is on the outside. Part three takes over and shows you what the hacker will do once they've gotten on, such as attacking other local users including root, and cracking passwords. It becomes obvious that you need to protect things from insiders as much as from the outsider, because the outsider will usually get in as a normal user first, and if you can prevent him or her from getting root access, the damage cannot be nearly as severe. A lot of books don't cover this angle at all, and it's done superbly here.Part four covers common problems in internet services. First they discuss mail servers. Sendmail, Qmail, Postfix, and Exim each get covered in detail - it's nice to see more than just Sendmail discussed in a security book. Of course, it'd be even nicer to see something other than Sendmail installed on a Linux machine by default. Next they cover problems with FTP software and problems with the FTP protocol. I'd never seen "beneath the hood" and realized how wierd FTP really was, and why it's not supported by firewalls very well, and the authors show you the inner workings of it so anyone can understand the problems. They continue with Apache and CGI/mod_perl/PHP/etc problems, both from a coding standpoint and how to secure against outsiders and your own web developers. Next it's on to Firewalls (iptables and TCP wrappers) and lastly (distributed) denial of service attacks. The countermeasures for the DOS problems are excellent, and a must for anyone with a server. Part five covers everything a hacker can do once they've broken in. They describe trojan programs, trojan kernel modules, and configuration changes that can be used to keep root access, or hide the hacker activity, or let them get back in should the computer be partially fixed. This was not only complete, but scary in how many different things they showed. It works both as a blueprint

for what you need to defend against, how to clean up after a hacker has gotten in, and also how you could back door a machine if you get in. I'll leave the ethics up to you. Lastly we have part six, which is the appendicies. While most times I ignore appendicies, these are really an integral part of the book, and are referenced throughout the book all over. (This very good, because it keeps the book from having too much repeated countermeasures.) They discuss post-breakin cleanup, updating your software and kernel, and turning off daemons (both local and network ones) and a new case study. The book is good about covering Linux from a distribution-agnostic standpoint (it doesn't assume you use RedHat, unlike everything else out there) but in these appendicies they cover the differences you may encounter. They show you how to use dpkg/apt-get as much as RPM as much as .tgz packages, discuss both inetd and xinetd, and even svscan/supervise. They are extreemly complete. Hacking Linux Exposed 2nd Edition is required reading for anyone with a Linux machine, period."

Hubert Dziedziczak, "A bit outdated information. Good book and contains a lot of useful information, however it a bit outdated."

The book has a rating of 5 out of 4.5. 39 people have provided feedback.

Book Information

Language: English
Paperback: 712 pages
Item Weight: 2.65 pounds
Dimensions: 7.25 x 1.5 x 8.75 inches