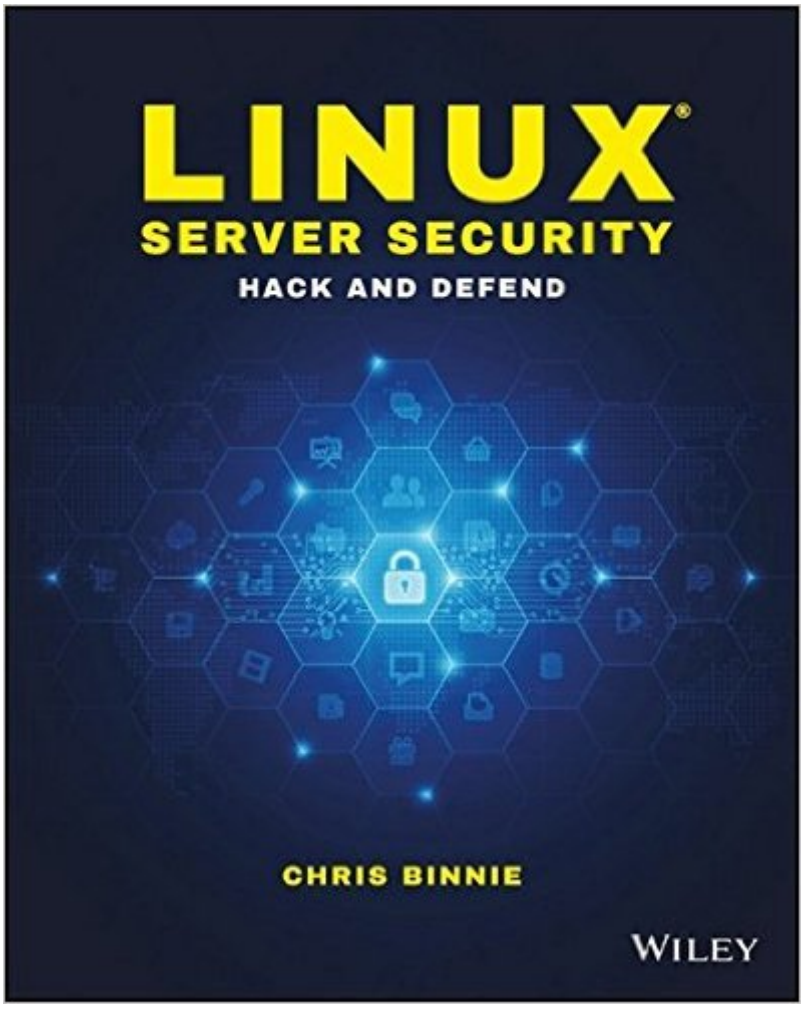
Linux Server Security: Hack And Defend



Synopsis

Learn how to attack and defend the worldâ ™s most popular web server platform Linux Server Security: Hack and Defend presents a detailed guide for experienced admins, aspiring hackers and other IT professionals seeking a more advanced understanding of Linux security. Written by a 20-year veteran of Linux server deployment this book provides the insight of experience along with highly practical instruction. The topics range from the theory of past, current, and future attacks, to the mitigation of a variety of online attacks, all the way to empowering you to perform numerous malicious attacks yourself (in the hope that you will learn how to defend against them). By increasing your understanding of a hackerâ ™s tools and mindset you're less likely to be confronted by the all-too-common reality faced by many admins these days: someone else has control of your systems. Master hacking tools and launch sophisticated attacks: perform SQL injections, deploy multiple server exploits and crack complex passwords. Defend systems and networks: make your servers invisible, be confident of your security with penetration testing and repel unwelcome attackers. Increase your background knowledge of attacks on systems and networks and improve all-important practical skills required to secure any Linux server. The techniques presented apply to almost all Linux distributions including the many Debian and Red Hat derivatives and some other Unix-type systems. Further your career with this intriguing, deeply insightful, must-have technical book. Diverse, broadly-applicable and hands-on practical, Linux Server Security: Hack and Defend is an essential resource which will sit proudly on any techie's bookshelf.

Book Information

Paperback: 144 pages
Publisher: Wiley; 1 edition (May 16, 2016)
Language: English
ISBN-10: 1119277655
ISBN-13: 978-1119277651
Product Dimensions: 7.4 x 0.3 x 9.3 inches
Shipping Weight: 0.3 ounces (View shipping rates and policies)
Average Customer Review: 3.6 out of 5 starsÂ Â See all reviewsÂ (5 customer reviews)
Best Sellers Rank: #1,289,261 in Books (See Top 100 in Books) #34 inÂ Books > Computers & Technology > Operating Systems > Linux > Servers #298 inÂ Books > Computers & Technology > Operating Systems > Linux > Networking & System Administration #674 inÂ Books > Computers & Technology > Internet & Social Media > Hacking

Customer Reviews

At barely over one hundred twenty pages Ã¢Â Âˆ Linux Server SecurityÃ¢Â Â™ should easily clear the first bar with its intended audience of admins and IT staff Ã¢Â Â“ itÃ¢Â Â™s compact enough to work through in a week or two of dedicated effort without feeling overwhelmed.The breakdown into ten tutorial-style chapters of 5-10 pages independent of sequence and content makes the book even more effective Ã¢Â Â“ the author encourages readers to pick and choose what most interests them and not worry about skipping what doesnÃ¢Â Â™t.A lot of Ã¢Â Âˆ hacker guidesÃ¢Â Â™ play coy by posing as white/grey hat when their authors and publishers know full-well their target readership is neither.But from the outset Binnie lays his cards on the table and the result is both educational for those curious about common types of server attacks and workplace practical for the professional looking to guard against them Ã¢Â Â“ and validate their defenses by trying out the attacks for themselves.The book assumes a good grasp of the command line Ã¢Â Â“ itÃ¢Â Â™s possible to simply type along and youÃ¢Â Â™ll certainly pick up syntax with patience and a good eye. But to focus of the essentials and get the most from the book you should be pretty fluent in shell scripting as well as networking and internet protocols Ã¢Â Â“ after all these are the primary avenues of attack described in the book.If thereÃ¢Â Â™s no preview above the following chapters each cover a form of attack and/or defense from one:Invisibility CloakDigitally Fingerprint Your FilesTwenty-First-Century-NetcatDenying ServiceNpingLogging ReconnoitersNmapÃ¢Â Â™s Prodigious NSEMalware DetectionPassword Cracking With HashcatSQL Injection AttacksIf all or most of the above draw a blank youÃ¢Â Â™re probably not in a position to gain the most from the book and IÃ¢Â Â™d recommend a more basic bookcovering network security issues and Linux admin.BinnieÃ¢Â Â™s writing is clear and lively. There are plenty of illustrations, script listings and snippets and the production value of the Wiley book is what youÃ¢Â Â™d expect: clean layout thatÃ¢Â Â™s very readable.Bottom Line: Plenty to learn here Ã¢Â Â“ presented in a no-fluff, detailed format thatÃ¢Â Â™ll enlighten interested readers, as well as shake loose some cobwebs in those who havenÃ¢Â Â™t taken server security quite as seriously as they should.

This is a rather thin book. It shows some good examples of Linux security with different tools, including knockd, ncat, nping, nmap, maldet, hashcat, etc.I was so underwhelmed by this book that if I had bought it, I would likely have return it because it provides very basic overview of these utilities. Each chapter is 3-4 pages and that includes a page that discusses history or background of how some of these utilities have evolved.What I really do not like is the fact that it simply repeats the basic commands on each chapter, like yum install, to fill up half of the page. If you remove the

history or background info, and the filler for repeated commands (yum, apt-get), this book would be even thinner so the actual substance in the book is really half of the 144 pages. That is very thin for a security book. When it introduces a new utility, like ncat, it does not go into any level of detail about it. So this book Ã¢Â Âœintroduces Ã¢Â Â• new Linux admin to some of these utilities and how they can be used, but doesn Ã¢Â Â™t go to the level of detail that intermediate to advanced Linux admins may expect.You will likely read this book only once. In other words, this book is not written like a reference book that you like to keep on your bookshelf that you know you will likely keep going back to. As long as you remember some of the commands and the context in which they were used, you will likely never go back to this book, even if you were a Linux newbie.

As author of Extending Jenkins and having worked with Chris in the past I was asked to review this book. The first thing that struck me is the diverse set of topics, and you are encouraged to delve deeper into those you find of most interest.The introduction talks about it being aimed at mid-level admins, but even as someone who has been in the industry for a long time I still found much of the content fascinating, thanks to the way in which it has been applied and explained by the author. The book could be longer but I found its quality made up for its page count.Technical authors sometimes forget that a cut and paste howto is not what you want from a book. Instead your want detailed commentary which you can reference again in the future. That generally only comes from an experienced and talented author, as Chris Binnie demonstrates here.

This is a concise and well organized read that I would certainly recommend to anyone delving into the world of Linux systems administration. Well worth purchasing for your reference collection, it succinctly covers a broad range of Linux server security areas. It serves as an excellent introduction to the massive topic that is system security, with no shortage of technical depth to explore. Even as a seasoned IT pro myself, I find this book a very useful reference point, to have to hand.

Basic security/hardening for linux.. you can get a better how-to from cisecurity free paper.

Server on a Global Network Hacking: Computer Hacking:The Essential Hacking Guide for Beginners, Everything You need to know about Hacking, Computer Hacking, and Security ... Bugs, Security Breach, how to hack) Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Defend Yourself: A Comprehensive Security Plan for the Armed Homeowner Linux Administration: The Linux Operating System and Command Line Guide for Linux Administrators CompTIA Linux+ Powered by Linux Professional Institute Study Guide: Exam LX0-103 and Exam LX0-104 (Comptia Linux + Study Guide) Linux Web Server Development: A Step-by-Step Guide for Ubuntu, Fedora, and other Linux Distributions Linux For Beginners: The Ultimate Guide To The Linux Operating System & Linux Linux Apache Web Server Administration (Linux Library) Linux DNS Server Administration (Craig Hunt Linux Library) Setting Up a Linux Intranet Server Visual Black Book: A Complete Visual Guide to Building a LAN Using Linux as the OS Hack a Wifi Network: Easy way to access Wifi Networks by using Linux os Hacking: How to Hack Computers, Basic Security and Penetration Testing The Curious Case of Kiryas Joel: The Rise of a Village Theocracy and the Battle to Defend the Separation of Church and State Negotiating with Backbone: Eight Sales Strategies to Defend Your Price and Value (2nd Edition) Negotiating with Backbone: Eight Sales Strategies to Defend Your Price and Value Honor and Defend (Rookie K-9 Unit)