Maximum Linux Security (2nd Edition)
Synopsis

Linux continues to gain acceptance as a high-level operating system that's ready for serious corporate enterprise-level computing. When running Internet or file servers, Linux is more reliable, more flexible, more cost-effective, and even faster in some cases than Windows 2000/NT. This means that more and more companies are running Linux on their Web and internal file servers, and that more and more network administrators, used to how things work on Windows 2000/NT servers, will need a crash course on the vulnerabilities of Linux systems, and which holes they're going to need to plug in order to protect themselves from outside attacks. Maximum Linux Security, Second Edition fills this need.

Book Information

Series: Maximum Security
Paperback: 896 pages
Publisher: Sams; 2nd edition (June 21, 2001)
Language: English
ISBN-10: 0672321343
Product Dimensions: 9.1 x 7.3 x 2 inches
Shipping Weight: 3.4 pounds
Average Customer Review: 4.3 out of 5 stars  See all reviews (12 customer reviews)

Customer Reviews

I am a senior engineer for network security operations. I read "Maximum Linux Security" (MLS) to learn more about defending Linux hosts in hostile environments (i.e., the Internet). Compared to recent editions of "Maximum Security," MLS is more useful and accessible. I recommend this book as a supplement to "Hacking Linux Exposed" and "Real World Linux Security."MLS is less list-oriented than the typical "Maximum Security" book. Useful advice on practical security measures takes the place of exploit listings. While you'll find discussions of older vulnerabilities, the most ancient are isolated in appendix B. The appendix also offers lengthy, detailed command listings and glossaries, unlike any I've recently seen. The friendly tone of the book reminded me of a mentor
speaking to a novice. Furthermore, the authors clearly know their material. For example, Linux frequently demands compiling tools from source code. Sometimes this process requires tweaking the code before running 'make’. The authors regularly give specific advice on the changes needed to get the code working properly. This attention to detail impressed me, and helped me run some of the example applications as I read the text. The authors also gave great clues on applying patches, a task required of every system administrator. Beyond its specific use as a Linux security text, MLS also lets readers learn of other resources useful to security practitioners. I was pleased to check out the Linux Cross Reference project, where I can browse and link to several incarnations of the Linux kernel. On the negative side, the back cover advertises MLS as an "intermediate-advanced" text.

I'll start off by saying that I am CISSP, CCSP and SANS GSEC certified. I have read a couple of the Maximum Security series books and I'm constantly disappointed. First off the book is about 5 times too long for a novice that is curious about the subject and under informative for a professional. It also seems to cover some "neeto" programs you can use to secure your system. For the amount of pages I thought it would at least delve into some kernel hacking, buffer overflow/underrun protection. The author seems to love to give scare tactic examples of attacks that happened years before the book was published. If someone is reading this book they most likely understand the threat. I don’t need to the police to tell me about murders that have gone on in Baltimore to convince me to put locks on my doors. This kind of off subject garbage makes this book even heavier, and not from an information stand point. Published in 2001 it seem that is was out of date then as well. It covers, for the lack of better description, low level hacker tools in a majority of descriptions of tools. For example the "Sniffer" chapter mentions nothing about dsniff a very popular and powerful sniffing utility. I would not recommend this book to a beginner as there is way too much garbage taking you through the installation of basic pieces of software. Never mentioning some different options maybe you should be selecting during the install. There is no need to cut and paste the contents of the INSTALL file from Tripwire, most of the guides for installing are word for word from the programs own install and readme files. I would not recommend this to a professional as well as it does not go into great enough detail about anything unless you don’t want to read man files and would rather have it in the form of a 13lbs book.

Download to continue reading...