

# BOOK REVIEWS

BY JAMES MOHR

## Linux Quick Fix Notebook

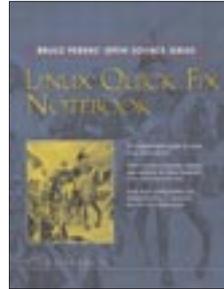
This book definitely caught me off guard. I know you can't judge a book by its cover, but I have grown weary of titles that have phrases like "power," "master," or "cookbook." So, when I got a copy of this "quick fix" book, I was naturally apprehensive. Looking through the table of contents, my apprehension was increased by the fact that the book covers all of the "standard" topics one finds in any book discussing Linux system administration. However, once I started reading, I was extremely impressed.

Despite my praises of this book, I think it a misnomer to use "quick fix" in the title, as this title implies a troubleshooting guide. Instead, the author goes to the heart of configuration and administration.

This book is for administrators, so you won't find "quick fixes" for things like

KDE or OpenOffice. Topics range from basic networking, through configuring Samba, to setting up a wireless network. The book covers web servers, performance, hardware, logical volumes, and much, much more. There were a number of places where I thought the author unnecessarily covered basic aspects of system administration (e.g., creating users). However, considering the size of the book and the amount of meat in the book, this problem was easily overlooked.

I do not want to say the book goes into a lot of detail. Instead, the author covers just the right amount of information to get the software working (often beyond the basics). Although the book covers a number of topics I won't ever use, I can't think of any topic I *will* use that wasn't addressed.



One thing that jumped out at me was the limited troubleshooting information for some topics. Some topics included substantial troubleshooting information, but in other cases, you are

simply told to check the appropriate log file. Despite this, the configuration steps sometimes included tips for what to look out for (perhaps making troubleshooting unnecessary). Plus, there were quite a few sections on testing the software, and these steps often also included common problems and their solutions.

**Peter Harrison**

**651 pages**

**Prentice Hall PTR, 0-13-186150-6**

**£ 24.99, US\$ 39.99, EUR 34.90**

## The Art of Computer Virus Research and Defense

The majority of the book addresses virus and other malicious code that is specific to Windows, so it might be a surprise that this book is being reviewed here. Most computer viruses are written for Windows simply because there are more Windows computers and Windows. Linux is not necessarily more secure – many of the problems discussed in this book can be used to attack Linux machines. Despite the emphasis on Windows, I found this book fascinating.

The book is written by Symantec's chief virus researcher, so you can be sure the author knows what he is talking about. If you

are interested in the history, philosophy, and physiology of computer viruses, this is definitely a book for you. Despite an occasional dry spot, I thoroughly enjoyed reading it.

The book is broken into two parts: "Strategies of the Attacker" and "Strategies of the Defender," addressing malicious code and what you to do about it.

The first part starts with a little history of computer science (such as Turing machines and Conway's game "Life"). It then goes into an overview of the various types of malicious code.

The remainder of the first part goes into the various ways malicious code can attack your system. Details of Windows and even DOS code are discussed

here. However, most of the concepts apply to any operating system, so it is just a matter of time before these concepts are applied to Linux. To get the most out of the code, you will need a basic understanding of x86 assembler.

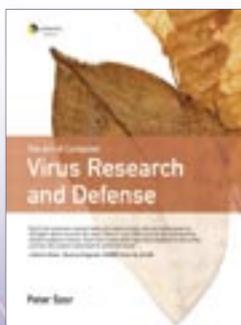
The second part of the books discusses techniques researchers use to identify and eliminate malicious code. You will also find information about what you can do at the administrative level to protect your systems, such as using access control lists, firewalls, and intrusion detection systems. All in all, this is a nice book to have.

**Peter Szor**

**713 pages**

**Symantec Press, 0-321-30454-3**

**£ 26.19, US\$ 49.99, EUR 43.50**



## Linux in a Windows World

This is definitely one of those “jump up and down” books. A number of books on “Linux-Windows integration” have appeared in the last few years, but none have impressed me as much as *Linux in a Windows World*. Other books try to provide a comparison of the features each operating system provides. This typically means the details of integration are left short-changed. Although the title might suggest a comparison, I found it refreshing that the book was not limited to simply comparing.

I was also impressed that the book did not fall into the trap of trying to fill pages with overly superficial descriptions of software products. There are a couple of exceptions, but for the most part, you are either given details of the product or simply told to look elsewhere. With close to 500 pages, the book is loaded with information, so I feel this approach is appropriate.

I found one of the most important aspects of this book was that it went beyond the issues of simple intergration. The term “intergration” is vague enough, and other books interpret it simply as meaning more or less having the two operating systems in the same network. *Linux in a Windows World* goes into a lot of detail about how Linux and Windows components *must* interact in order to work correctly.

The book provides a whole chapter on accessing Windows applications from Linux, and vice versa. For

example, running an X server on your Windows machine to access Linux apps, or using *rdesktop* on your Linux machine to access Windows. There is also a chapter on “Remote Text-Mode Administration and Use.” Although this is a short chapter, I found

it very useful for environments that do not allow GUI access. This configuration is common in high security environments like the one where I work.

The book also goes beyond simple integration in its

discussion of the issue of *replacing* Windows with less expensive Linux systems.

Although the book does not give step-by-step instructions, there is a great deal of information on configuring Linux to provide the functionality previous provided by Windows.

I did find a couple of places that I felt were too far afield from the topic of “Linux-Windows integration,” such as details of spam assassin or configuring *tar* for local backups in Linux. Still most of the information was useful, regardless of whether you were trying to integrate Linux and Windows.

Like most new O’Reilly books, *Linux in a Windows World* comes “Safari Enabled,” which means you have 45 days of free access to the online version of this book. O’Reilly has another winner with this one.

**Roderick Smith**  
**478 pages**  
**O’Reilly Media,**  
**0-596-00758-2**  
**£ 35.50, US \$44.95,**  
**EUR 39.50**

