BOOK REVIEWS

BY JAMES MOHR

Forensic Discovery

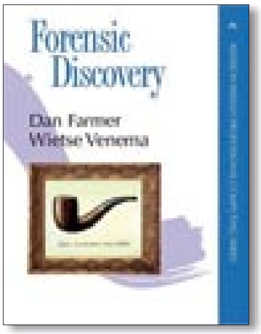
Although *Forensic Discovery* does not start with "It was a dark and gloomy night," it has the feeling of a classic murder mystery, where the detective collects single stands of hair from the crime scene to find the murderer. Like a crime thriller, this book is primarily focused on collecting and analyzing information.

The book is written by two of the most well-known computer security experts. However, unlike other books I have read by a so-called experts, this one is enjoyable to read. The authors make a potentially dull subject actually very exciting.

The book starts with basic concepts and issues without going into details. Most of what is presented is logical. I personally never thought much about many of these issues and thus suffered from some of the same problems the authors discuss. For example, one of the basic principles of forensics, whether related to computers or not, is the fact that the act of collecting evidence often influences or even *destroys* the evidence you are trying to collect (for example, DNA testing of blood samples). In a computer context, it is a common practice to make backups of log files that can end up destroying important information such as the last access time (which is often a useful piece of the puzzle).

The book goes into a lot places that many (if not most) system administrators overlook. The authors get beyond the theoretical question of where one *might* look for information and show real examples of places where useful clues may lie hidden.

After you have discovered a break-in, the next step is to determine if the intruder left anything behind, particularly something like a root kit that will provide access to the system. The trail goes beyond simple open ports or replaced binaries. The authors even discuss how to determine if the intruder has made changes to the kernel.



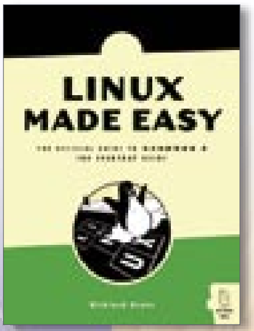
This kind of book has to reveal tools and methods used by the bad guys. In doing so, the authors may be giving new ideas to would-be intruders. Every system administrator should read this book before the bad guys do.

Dan Farmer and Wietse Venema
217 Pages
Addison-Wesley, 0-201-63497-X
£ 28.99, US$ 39.99, EUR 36.90

Linux Made Easy

Admittedly, this book was my first introduction to the Xandros Linux distribution. This introduction was made easy by the copy of Xandros (Open Circulation Edition) included with the book and even easier by the author's style of writing.

Rickford is obviously both a Linux and a Xandros fan, but he does not come across as someone who says these are the *only* things you should be using. Instead, he presents the material as one alternative, even explaining how to dual boot Linux and Windows.



One nice feature of the book is the projects that appear throughout the text. These step-by-step procedures cover various tasks, ranging from adding fonts to working with OpenOffice.

Having started with Linux at a time where the easiest way to install was using floppies, I *might* be tempted to ding the book because of the limited coverage of administration topics. However, Linux has reached the stage where it is as easy to install and use as Windows, so you don't need as many administration topics in end-user books. However, the author does go into the "administration" of commonly used hardware like sound cards, TV tuners, printers, and so forth.

Although the tasks tend to get more difficult as the book progresses, I wouldn't say that reading it in sequence is required. Instead, you can jump in anywhere. The author emphasizes some of the most common applications of the Linux desktop, including productivity applications, games, and even some educational software.

This book definitely shows that Linux is (finally) easy-to-use. It is no longer a "hacker's OS."

Even having used Linux for as long as I have, I did learn a fair bit about some of the applications. For a beginner, particularly if you are using Xandros, this is definitely a "must have."

Rickford Grant
459 Pages
No Starch Press, 1-59327-035-6
£ 19.52, US$ 34.99, EUR 32.50