# book reviews

Reviewed by Rik Farrow

## NETWORK SECURITY HACKS

Andrew Lockhart

Sebastopol, CA: O'Reilly, 2004. Pp. 298.
ISBN 0-596-00643-8.

The latest in the series of "Hack" books, *Network Security Hacks* provides you with 100 mini-security lessons in how to use security tools and techniques. I liked the book, as I find there is always something new to learn, and the Web is not always the best place to find out how a tool works.

I found most of the hacks clearly written, with enough examples to explicate the descriptions. Occasionally, I would discover a subtlety that might confound the naive user: for example, instructions for setting up SSH port forwarding that simply assume that the reader knows that the other end of the connection must already be running an sshd.

Still, I really appreciate the work that went into the hacks. The format makes it easy to pick the book up when you have less than an hour to try to improve your skills or learn how to use an unfamiliar tool. There is a lot that will be familiar to expert sysadmins, but for a beginner-to-intermediate sysadmin, there's lots to learn here.

## KNOW YOUR ENEMY: LEARNING ABOUT SECURITY THREATS, 2D ED.

The Honeynet Project

Boston: Addison-Wesley, 2004. Pp. 740.
ISBN 0-321-16646-9.

This is the second edition of the Honeynet Project's opus, and I was interested in seeing what had been added. If you follow the Honeynet Project closely, a lot will be familiar. But the second half of the book contains forensics case studies that will alone be worth the purchase price for many readers.

The Honeynet Project began in 1999 as a loose collaboration of security researchers. They began to collect information about hacking techniques by setting up networks containing honeypots, systems intended to be attacked. Over time, their techniques have improved, making their honeynets more useful as they became easier to set up.

I was most interested in the case studies in later chapters of the book. Careful explanations of how to diagnose hacked systems are both useful and rare. I especially enjoyed reading about just how much work went into decompiling a binary attack tool. I teach the basics of understanding how to assess a hacked system, but the book goes a lot deeper than I have time for.

If you want to learn about practical computer forensics, there is a wealth of material in this book. Based on real-life experience, this book is the one you want if you are permitted to diagnose one of your own systems after it has been hacked. Ideally, you will use the examples on the included CD-ROM before that occurs.

## MAC OS X: THE MISSING MANUAL

David Pogue

Sebastopol, CA: O'Reilly, 2003. Pp. 762.
ISBN 0-596-00615-2.

The mere size of this book hints that there is a lot missing from the OS X online help system—and I'm not just joking about the security hole discovered in May 2004. This *Missing Manual* has already proven its worth more than once for both me and my wife.

When I bought a G5 in 2003, I set it up in my office and started configuring it. At first I thought, "This is a no-brainer!" Installing software packages from CDs went smoothly, as did configuring the G5 with static IP addresses. But then I needed root, and found it wasn't there. Well, there is a root account in MacOS X; you just need to know how to enable it. *The Missing Manual* provides step-by-step instructions, as well as important warnings about why you don't want to use the root account and a recommendation to use sudo instead.

In another test of usability, Pogue's book passed one of the hardest tests I could imagine. I had set up an account on the G5 for my wife. Part of the reason I got a G5 was that I was tired of re-installing Mac OS 9, as it would get corrupted within a couple of weeks. Now my wife could use my G5, and I could manage it using a terminal window. Well, not quite.

First, my wonderful wife managed to rename her Library folder, which has immediate and dire consequences. She really didn't even know that was what she had done, but I needed both Pogue's help and the root account to fix the problem.

But that was not the acid test. I put *The Missing Manual* by the G5 and suggested that my wife try reading the manual instead of automatically asking me questions. Not only did she read the manual, but she learned how to use the OS X calendar tool with the help of the book. She has continued to use *The Missing Manual* to learn about the Mac and to solve other problems on her own. (I still get to help with the more mysterious issues.)

*The Missing Manual* is clearly written and works for both technical and nontechnical users. I can highly recommend this book.