book reviews

RIK FARROW

rik@usenix.org

USENIX would like to thank Æleen Frisch for taking over the "Bookworm" column from Peter Salus on short notice. *;login:* is changing, and the "Bookworm" column is morphing into a new book reviews section, with detailed book reviews included in each edition of *;login:*. The new book review section will appear in the October 2005 issue.

ADVANCED PROGRAMMING IN THE UNIX ENVIRONMENT, 2ND EDITION

Richard Stevens and Stephen Rago

Addison-Wesley, 2005, 0-201-43307-9, 800 pp.

If you do any UNIX programming, or Linux or MacOS programming, this is the book you want to keep handy. The first edition, by Rich Stevens, became an instant classic for good reason. Stevens provided clear and detailed examples of how to use the many system calls provided by the UNIX programming environment of the day (that edition was published in 1992). But things have changed. The second edition, written by Rago, covers currently popular operating systems: FreeBSD, Linux, Solaris, and Darwin (MacOS X). The second edition also includes new topics, such as threading and multithreaded programming, as well as other things that were less common 13 years ago, like networked printers and the Web.

You might be tempted to believe that this book isn't necessary. After all, you have the Web at your fingertips, with a wealth of software to copy and resources to read. Not very long ago, I found myself wanting to collect the IP address of a client as it connected to a server I was writing for one of my classes. I started searching for a good, yet short, example of the code I needed. And never found it.

The second edition explains exactly how to get the IP address from a connecting client, and how to convert it into a human (person) readable format using inet_ntop(). What I spent hours struggling with on the Web was easy with this book.

I used the previous edition as an important reference, but had misplaced it (too many bookshelves). Now, the second edition sits by my desk ready to lend assistance as soon as I need it. I can highly recommend this book. Rago has carried on in the fine tradition of Richard Stevens.

MASTERING FREEBSD AND OPENBSD SECURITY

Yanek Korff, Paco Hope, and Bruce Porter

O'Reilly Media, Inc., 2005, 0-596-00626-8, 445 pp.

I found that this book reminded me of Mick Bauer's *Linux Server Security*, in that it begins with some hardening and administration basics, then continues with installing and securing common services (mail, DNS, and Web). The authors have produced a clearly written book that is authoritative and contains easy-to-follow instructions. That the instructions are tailored specifically to the two most popular BSD distributions is a big help. You are told how to find the right version of the DNS server software (whether from ports or elsewhere), how to build it, and how best to configure it.

I consider this book a fine addition to my security shelf, and have already used it to tweak the security of my DNS server.

LINUX NETWORK SECURITY

Peter Smith

Charles River Media, 2005, 1-58450-396-3, 541 pp.

You might think that I would be satisfied with Bauer's book, but Smith's book forms a fine complement to it. Unlike *Linux Server Security*, Smith's book starts off with a section about network-based attacks. Bauer's book does discuss using netfilter, but Smith's goes into much greater detail on using iptables, making it a better all-around reference for this topic. Securing services are a minor topic here. Instead, there is a lot of material about choosing a Linux distribution and the various add-ons for increasing the security of the system. I really like the chapter on hardening, especially the parts that explain the various memory (buffer overflow) protection schemes that work in Linux.

There is an entire chapter devoted to explaining and contrasting the various access control solutions for Linux (such as SELinux, GRsecurity, and LIDS). This book would be a complete Linux security book (instead of network security) if there were a bit more detail (there are only two paragraphs) about file and directory permissions. The rest of the "Basic System Security Measures" chapter does measure up to what I would expect from a book on Linux security. I recommend that this book serve as a textbook for classes in Linux security, or for anyone who wants a serious reference work on current Linux security features.