ÆLEEN FRISCH

the bookworm

Æleen Frisch is a system administrator and writer living in Connecticut (www.aeleen.com).

aeleen@usenix.org

Books Reviewed in this Column

FORENSIC DISCOVERY

Dan Farmer and Wietse Venema

Addison-Wesley, 2004, 0-201-63497-X, 217 pp.

BUILDING A LOGGING INFRASTRUCTURE

Abe Singer and Tina Bird

Short Topics in System Administration 12, USENIX Association, 2004, 1-931971-25-0, 82 pp.

TROUBLESHOOTING LINUX FIREWALLS

Michael Shinn and Scott Shinn

Addison-Wesley, 2005, 0-321-22723-9, 381 pp.

INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS

Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher

Prentice-Hall, 2004, 0-13-147573-8, 400 pp.

THE EXECUTIVE GUIDE TO INFORMATION SECURITY: THREATS, CHALLENGES, AND SOLUTIONS

Mark Egan with Tim Mather

Addison-Wesley Symantec Press, 2005, 0-32-130451-9, 288 pp.

SLAMMING SPAM: A GUIDE FOR SYSTEM ADMINISTRATORS

Robert Haskins and Dale Nielsen

Addison-Wesley, 2005, 0-13-146716-6, 420 pp.

SENDMAIL MILTERS: A GUIDE FOR FIGHTING SPAM

Brian Costales and Marcia Flynt

Addison-Wesley, 2005, 0-321-21333-5, 347 pp.

LINUX APPLICATION DEVELOPMENT, 2ND EDITION

Michael K. Johnson and Erik W. Troan

Addison-Wesley, 2005, 0-321-21914-7, 732 pp.

JAVA APPLICATION DEVELOPMENT ON LINUX

Carl Albing and Michael Schwarz

Prentice-Hall, 2005, 0-13-143697-X, 598 pp.

KNOPPIX HACKS: 100 INDUSTRIAL-STRENGTH TIPS & TOOLS

Kyle Rankin

O'Reilly, 2005, 0-596-00787-6, 314 pp. + CD.

I am thrilled and honored to be taking over from the illustrious Peter Salus as the Bookworm. This month's books are a somewhat random set, as the review copy pipes are just getting started for me.

FEATURED: *FORENSIC DISCOVERY*

Dan Farmer and Wietse Venema are best known collectively as the authors of the SATAN security evaluation application. However, they are also the authors of the one of the most important security articles in the literature, "Improving the Security of Your Site by Breaking into It," which explained the concept of (implicit) transitive trust. Venema and Farmer have collaborated on a new software tool, the Coroner's Toolkit, for performing post-break-in analysis; this is also the subject of their new book (the software appears at various points throughout the book and is discussed in an appendix). The book is divided into three parts, covering an overview of forensics and related concepts, fundamental system entities/data structures related to forensic discovery, and the specifics of data persistence.

This book is an excellent mix of the theoretical and the practical. Fundamental concepts are covered in detail, as are system data structures and entities (e.g., file systems, inodes, processes, system calls), providing a helpful—and necessary—knowledge base for the specific techniques for examining the latter that follow. As is typical of their work, Farmer and Venema have the knack of getting even experienced UNIX folks to look at and appreciate familiar things/material in a new way.

A significant thread running through the book is the persistence of data, including data deleted from memory and storage media. In the first chapter of the book's final part, the authors have compiled and performed a number of useful experiments that enable them to make very specific quantitative statements (e.g., how long trace data from a deleted file can be expected to linger under various system usage scenarios). This kind of information is needed to make both analysis and prevention planning practical (or even feasible).

This book is extremely useful for a wide spectrum of readers. People who are just getting started with computer forensic analysis will find it a clear and useful first book that will provide additional benefits on rereading. At the other extreme, experienced security administrators will appreciate the authors' clarity and insight in thinking about forensics in general and the specific discovery/analysis operations in particular. I always find that reading Dan and Wietse's work inspires me to strive for greater excellence in my own.

THE DEFINITIVE WORK ON LOGGING

Abe Singer and Tina Bird have done a marvelous job with the latest volume in SAGE's Short Topics in System Administration series. *Building a Logging Infrastructure* is a very comprehensive discussion of syslog and its uses and foibles. The work covers logging on both UNIX/Linux and Windows systems, and also discusses some replacements for syslog and when they are useful or necessary. The relative lack of material on log data reduction is due to the dearth of options in this area rather than the authors' omission. This book is so good that I find myself falling into a typical writer's emotional pitfall: being jealous that I didn't write it myself. A must-have for everyone.

THREE MORE ON SECURITY

The authors of *Troubleshooting Linux Firewalls* describe their books as including "the Tao of firewall security, the Zen of troubleshooting, and the nitty-gritty step-by-step instructions to fix a problem." This is a good description of their approach to their topic. The book does a very good job of handling the second and third of these items, which is the main thrust of their book. The first topic, firewall security, covered in two early chapters, seems a bit rushed (more space needs to be given to system hardening in particular). The book focuses on RedHat and SuSE Linux, but the principles and many of the specifics apply to almost any Linux distribution.

Internet Denial of Service: Attack and Defense Mechanisms is an in-depth treatment of DoS and DDoS attacks and ways of responding to and preventing them. The authors constitute a DoS dream team. Not surprisingly, the level of detail, understanding, and technical expertise is consistently high throughout the book. The book is also quite readable and even in tone and quality, despite having four authors. Don't let the book's goofy cartoon cover illustration mislead you or put you off. This is a serious book on an important topic.

Finally, *The Executive Guide to Information Security* is exactly what it sounds like: a book about computer security designed for nontechnical business executives. It places security concepts and practices within a typical business framework (mindset). As such, it may be useful to some readers of this column who need to present such technical information to managers and other nontechnical audiences.

SPAM IS THE WORD

Slamming Spam is another excellent book. It surveys all of the major spam-fighting techniques in common use today, covering both user-level and system-level strategies. It discusses—and provides detailed, correct directions for—configuring email clients ("user agents"), Sendmail, Postfix, qmail, Exchange, and Lotus Notes for spam filtering. It includes chapters on procmail, SpamAssassin, Vipul's Razor, blacklists, SMTP authentication, sender verification, and, of course, Bayesian filtering. Mail administrators, system administrators, and anyone who has to deal with a significant spam problem will find this book indispensable.

Sendmail Milters is the definitive reference for using Sendmail's filtering facility—milters—for dealing with spam messages. Its four parts cover the characteristics of spam, deploying a test environment for developing and testing, writing milters, and configuring Sendmail to use milters. This book is very comprehensive, extremely well written and eminently readable, and of the high quality one would expect from Brian Costales, working in concert here with Marcia Flynt.

A PAIR ON LINUX PROGRAMMING

Both of the programming books this time are aimed at beginners of various sorts. *Java Application Development on Linux* is written for readers with some programming experience and a basic familiarity with object oriented programming concepts. The first major section of the book introduces the Linux environment and the basic Java language, and the remaining four parts cover Java in action, including database queries, GUIs, Web interfaces, and distributed applications. The pace of the book is slow, but this is appropriate for its intended audience, and the book is long enough to introduce its topics in nontrivial detail. Students—and others—with only a moderate amount of programming experience will have no trouble working through this book on their own, and they'll be ready for advanced Java texts when they are through.

Linux Application Development is now in its second edition. Peter called the previous edition "a superb piece of work," while noting that it "makes no concessions to the unwashed." It would seem that much of the effort that went into the second edition was designed to broaden the book's appeal. For example, it now provides many, albeit brief, explanations of how Linux does things and also includes coverage of glibc. The book has been updated for the 2.6 Linux kernel and GNU C library 2.3. It continues to serve as an excellent reference for serious Linux application developers.

PARTING GLANCE

I'm going to try to end each column with a brief mention of something a little out of the mainstream. This time it's *Knoppix Hacks*, a book that made me nostalgic for the days when I frequently used a Yggdrasil install CD as a PC hardware diagnostic tool. Knoppix is a Linux distribution that runs directly from a CD without installation to disk. This book describes the many tasks it can perform, ranging from system configuration and repair to creating computer kiosks and roll-your-own Tivo-like systems. My one gripe with the book is its organization. Like all of the volumes in the O'Reilly Hacks series, it is structured as a numbered series of short articles, a scheme that inevitably favors breadth over depth. I'd say about two-thirds of the topics here are useful and the other one-third are cool, resulting in a book that is a good reference and also fun to flip open and start reading.