;login:

THE MAGAZINE OF USENIX & SAGE

October 2002 volume 27 • number 5

inside:

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

the bookworm

BOOKS REVIEWED IN THIS COLUMN

HACKER'S DELIGHT

Henry S. Warren, Jr.

Boston, MA: Addison-Wesley, 2002. Pp. 306. ISBN 0-201-91465-4.

UNIVERSAL COMMAND GUIDE

Guy Lotgering & the UCG Training Team

New York: Hungry Minds, 2002. Pp. 1591 + CD-ROM. ISBN 0-7645-4833-6.

ABSOLUTE BSD

Michael Lucas

San Francisco: No Starch Press, 2002. Pp. 616. ISBN 1-886411-74-3.

SENDMAIL PERFORMANCE TUNING

Nick Christenson

Boston, MA: Addison-Wesley, 2002. Pp. 228. ISBN 0-321-11570-8.

ECONOMETRICS, VOL. 3.

Dale W. Jorgenson

Cambridge, MA: MIT Press, 2002. Pp. 461. ISBN 0-262-10094-0.

THE COMMUNICATIONS TOOLKIT

P.H. Longstaff

Cambridge, MA: MIT Press, 2002. Pp. 271. ISBN 0-262-12246-4.

THE ESSENTIAL GUIDE TO NETWORKING

Jim Keogh

Upper Saddle River, NJ: Prentice Hall, 2001. Pp. 407. ISBN 0-13-030548-0.

THE PRACTICAL SQL HANDBOOK, 3RD ED.

J.S. Bowman et al.

Reading, MA: Addison-Wesley, 1996. Pp. 454. ISBN 0-201-44787-8.

ORACLE WEB APPLICATIONS

Andrew Odewahn

Sebastopol, CA: O'Reilly, 1999. Pp. 256. ISBN 1-565-92687-0.

XML AND SQL SERVER 2000

John Griffin

Indianapolis, IN: New Riders, 2001. Pp. 384. ISBN 0-735-71112-7.

WEB DATABASE APPLICATIONS

Hugh E. Williams & David Lane

Sebastopol, CA: O'Reilly, 2002. Pp. 582. ISBN 0-596-00041-3.

by Peter H. Salus

Peter H. Salus is a member of the ACM, the Early English Text Society, and the Trollope Society, and is a life member of the American Oriental Society. He is Chief Knowledge Officer at Matrix NetSystems. He owns neither a dog nor a cat.

peter@matrix.net

This is going to be a strange, disjunctive column.

I was going to rest a bit and write about the SQL books I've been looking at since June. But a number of things have hit my mailbox, and the SQL stuff will just take some space at the end of this piece.

There are five books I really enjoyed this past few weeks. One of them is a little out of line, but I think worthwhile. The others are obvious choices.

Hacking

Hank Warren has been hacking for about 40 years. In that time he has come up with a number of neat ways to do math and some algorithms that are quite useful.

Hacker's Delight is, to me, the computenik's response to W.W. Sawyer's *Mathematician's Delight*, which I discovered when I was in high school. Warren has made the world of elegant and efficient hacking come alive, and has managed to be useful at the same time.

Commands

The Universal Command Guide weighs in at about 4 kilos. It may be the most unreadable book I've got; but it's also the most useful one I've seen.

Every command for Windows 95, 98, Me, NT 4.0, 2000, XP; Solaris 7.8; AIX 4.3.3; OpenBSD 2.7; RedHat Linux 7; NetWare 3.12, 4.11, 5.1.6; Mac OS 9.1; and DOS 6.22 is listed. Over 8000 of them. And they're indexed and cross referenced.

The CD-ROM is very well done, and the indexing is superb. You may not need this tome, but you do need the CD.

FreeBSD

I read most of *Absolute BSD* on my flight home from the security symposium. A very fine piece of work, it isn't about how to implement BSD solutions, but it is about managing systems in situ. Its big lack is that there's no bibliography.

Sendmail

Christenson has not written an ordinary book. This is a book for the sysadmin who spends a lot of time working on her mail servers. UNIX mail servers. All over the world, more mail servers run Sendmail than anything else. About 15 years ago, I looked at the `sendmail.cf` file running on our Sun 3/150. I hope to never have to look at one again.

Featuring Sendmail 8.12, this book may possibly enable me to never look at one again. It is not a replacement for Costales and Allman (1997), but if you meddle with mail servers, you need this volume.

Hard-Core Economics

Dale Jorgenson is a professor of economics at Harvard. But don't let that or the fact that his subject is supposed to be tedious put you off.

Econometrics 3 is the third volume of Jorgenson's papers. It is subtitled "Economic Growth in the Information Age." I was really taken by a number of the articles in this hefty book: "Information Technology and the US Economy" and "Computers and Growth" serve as a great introduction to Jorgenson's interests. "What Ever Happened to Productivity Growth?" and "Did We Lose the War on Poverty?" were really enlightening.

book reviews

Two Other Good Books

While I'm on a roll, I want to tip my hat to P.H. Longstaff, whose interests are in communications business and policy. As we recognize that computers (and the Internet) are a part of that communications business, it becomes ever more necessary to try to understand it. *The Communications Toolkit* does a really good job of providing the flexible strategies we'll need in the future.

Keogh's book is the best introduction to networking for your grandmother I've come across. It is so simple and straightforward that even politicians should be able to comprehend it. At times Keogh dumbs things down a great deal, but this may be necessary.

SQL

After I read the Sleepycat BDB book, I realized that I needed to know more about SQL and its uses. I looked at and read too many items. But here are the four that I found most useful.

Bowman and her colleagues produced their volume over five years ago. Though there are some parts that are dated, I think it may be the very best book I've seen on SQL.

Odewahn's book is also a bit dated, but it is both clear and well written. The early chapters are a bit too introductory, but the final four were very, very good. On occasion, I wanted a bit more detail, though.

Griffin's book is far more up-to-date. It's good, with many useful examples.

Williams and Lane is also good, especially the PHP and MySQL sections. I can recommend all four.

INCIDENT RESPONSE:
A Strategic Guide to Handling System and Network Security Breaches

Eugene Schultz and Russell Shumway
New Riders Publishing, ISBN 1-578-70256-9

Reviewed by Anton Chuvakin
Anton Chuvakin, Ph.D., GCIA, is a senior security analyst with a major security company.

anton@netForensics.com

Incident Response by Eugene Schultz and Russell Shumway – the third book with this title that I have reviewed – had to overcome a certain expectation barrier, even though the authors are recognized experts in the security field. It passed the barrier with flying colors, being different but still covering many facets of the intricate incident response (IR) process, with sections on technology, procedures, and, especially, people.

The books starts with security basics. A risk assessment overview with loss estimates and a summary of digital risks (such as privilege escalation, break-in, denial-of-service, etc.) is provided. This material appears to be useful mostly for newcomers to the security field. Formal six-stage incident-response methodology is then presented by the authors: the preparation, detection, containment, eradication, recovery, and follow-up (PDCERF) process helps create a solid skeleton to support the fluid form of the IR process.

Admittedly, the book is less hands-on oriented than some other IR manuals; the reader will not find things like computer forensics-tool command-line options and ext2fs file system internals here. However, the book shines in its coverage of the human aspect of incident response. Written by an ex-CIA Ph.D. psychologist, the amazing chapter on social sciences and incident response covers a diverse range of topics: cybercrime profiling techniques, such as victim counseling and victimology; "modus operandi" identification; attack pattern recognition; establishment of threat level and communication with attackers. The chapter provides an exciting journey into the mind of a computer criminal, a cyber-sleuth, and a cybercrime victim. Also covered are insider attacks, often considered to be the doom of information security. The question "Why do insiders attack?" is thoroughly analyzed. The author overlays social methods on standard incident-response procedure (detection/containment/eradication/rec overy) to help understand the crucial role the human element plays in any security incident.

Two chapters are devoted to high-level computer forensics overview. Hard disk basics are explained – FAT, cluster, secure deletion are all given appropriate space. The book goes on to talk about the "guiding principles" of the investigation. A brief overview of forensic software and hardware is also provided but only serves to familiarize the reader with the names of common packages and utilities. For example, TCT coroner kit is only given about 15 lines of text.

Honeypots also take an honorable place in the book. Their role in IR is studied in detail and is deemed important. Honeypots are also tied to PDCERF, and their value in studying attackers, shielding IT resources, and even gathering evidence for court prosecution is recognized. Some common ways of implementing honeypots (such as via virtual environment) are discussed. The authors even digress to touch upon the ethical implication of honeypots.

Another gem is a stimulating chapter on future directions in IR. The ambitious prediction of intelligent automated incident response and attacker tracking tools is made by the authors. While it is known that automated response to security incidents must be viewed with caution, the potential seems to exist for future automated IR "helpers."

book reviews

An overview of legal issues is a must for any IR book. A brief and to-the-point section on US laws and international cybercrime treaties is available.

Last but not least, a short response and reporting checklist is compiled by the authors. It is based on the six-step IR process and will help investigators to structure their efforts and assist with data collection. Also included is a copy of a "Site Security Handbook" (RFC2196), with an extensive list of references.

Overall, the book is an extremely useful guide for security managers and those tasked with organizing/maintaining incident response teams. Skilled computer crime investigators will not learn anything new from this book, but they will likely enjoy the book nevertheless.

HONEYPOTS: TRACKING HACKERS

Lance Spitzner
Addison Wesley Professional,
ISBN: 0-321-10895-7, 480 pp.

Reviewed by Anton Chuvakin

If you liked *Know Your Enemy* by the Honeynet Project, you will undoubtedly like Honeynet Project founder Lance Spitzner's *Tracking Hackers* much more. In fact, even if you did not like *Know Your Enemy*, you will probably be impressed with the new book on honeypots and their use for tracking hackers.

The structure of the book is different from *Know Your Enemy*: Spitzner begins with his first honeypot penetration experience and goes on to talk about all aspects of honeypots. In-depth and structured background on honeypot technology is provided. Honeypots are sorted by the level of interaction with the attacker they are able to provide.

In addition, the book covers the business benefits of using honeypots. By classifying honeypots by their value in the areas of prevention, detection, and response (exactly as done in Honeynet Project white papers), Spitzner analyzes honeypot technology's contribution to an overall security posture. He also describes the differences between research and production honeypots and demonstrates the benefits of both for various deployment scenarios.

A large part of the book is devoted to particular honeypot solutions – "honeyd" by Niels Provos, plus several commercial honeypots – with detailed explanation of how they work. For example, there is a clear description of ARP spoofing and how it is used by the "honeyd" honeypot daemon. An interesting chapter on "homegrown" honeypot solutions (such as the ones used to capture popular worms of 2001) sheds some light on the simplest honeypots that can be built for specific purposes, such as one to capture a popular attack by means of a simple port listener. Use of a UNIX `chroot()` jail environment for honeypots is also analyzed.

Of course, a special chapter is devoted to honeynets, Honeynet Project's primary weapon in the war against malicious hackers. Generation II honeynet technology is introduced in the book. The chapter not only lists honeynet deployment and maintenance suggestions but also talks about the risks of honeynets.

Another great feature of the book is a chapter on honeypot implementation strategies and methods, such as using NAT to forward traffic to a honeypot and DMZ honeypot installation. The information is then further demonstrated using two full honeypot case studies, from planning to operation.

What is even more important, maintaining the honeypot architecture, is covered in a separate chapter. Honeypots are a challenge to run, mainly since no "lock it down and maintain state" is possible. One has to constantly build defenses and hide and dodge attacks that cannot be defended against.

Tracking Hackers also has a "Legal Issues" chapter, written with a lot of feedback from a Department of Justice official. It dispels some of the misconceptions about honeypots, such as the "entrapment" issue, and summarizes wiretap laws and related data-capture problems.

The book is almost the cutting edge of honeypot research and technology; to truly get the cutting edge and learn about the Honeynet Project's latest activities in detail, wait for the second edition of *Know Your Enemy* (coming out next year). In the "Future of Honeypots" chapter, Spitzner includes material on honeypot-based early warning system and distributed deployments, analysis of new threats, expanding research applications, and making honeypots easier to deploy and maintain.

To conclude: Marcus Ranum's enthusiastic preface is not an overstatement. It is indeed a great book, both for security professionals and for others interested in this exciting technology. While I was already familiar with most of the information in the book, it was a fascinating read! This book is a real page turner.