book reviews

INCIDENT RESPONSE & COMPUTER FORENSICS, 2D ED.

CHRIS PROSISE, KEVIN MANDIA, AND MATT PEPE

McGraw-Hill Osborne Media, 2003 Pp. 507.
ISBN 007222696X.

REVIEWED BY ANTON CHUVAKIN

Incident Response is back with a vengeance! I should disclose that I was very impressed with the first edition, for many reasons. Most of the points I liked about it are still valid, and new ones abound.

As before, the book is a great combination of high-level policy and methodology material with hands-on "hex dumps and disk images" stuff. The focus is on tools and technology as well as on the process of response and forensics.

The authors cover incident response process in great detail: from policy to secure and auditable host configuration, system logging, network monitoring, and evidence acquisition on multiple platforms. In fact, I liked the balanced platform coverage of both UNIX/Linux and Windows. The book also contains a lot of neat background material on TCP/IP and filesystems, making the book useful for the less security-savvy.

The useful distinction between first response and investigation is outlined. The reader will know what to do when confronted with a freshly hacked box and will also learn how to approach a hard disk extracted from the workstation of a dishonest employee. So, both cursory and in-depth response are covered.

I also enjoyed network-based-evidence chapters on monitoring and traffic analysis (using tcpdump, ethereal, tcpflow, tcptrace). Overall, the data analysis chapter was the most fun for me. Also enlightening were the chapters on evidence collection and preservation methods. To navigate the maze of what is allowed and what is not, – get the book.

Another awesome chapter was the one on reversing and hostile binary analysis. While not comprehensive, it seem to summarize the "busy man's reversing tips," applicable in daily security practice.

The main advantage of the book, in my opinion, is its comprehensive nature. It is both a practical "how to" guide and a good reference for "what is out there." The book conveys the sense of having been written by people who actually did all the things described in it. It might sound strange, but I also appreciated the lack of a "legal material" chapter. Legal advice should be heard from a lawyer and not from a security book (and is usually extremely boring anyway).

Is It 10 Years Already?

by Peter H. Salus

I'd like to celebrate February 4, 1994. Here's why.

At every USENIX meeting from 1986 on, Keith Bostic would stand up and announce that "35% of the CSRG's programs are AT&T code free"; "55% . . ."; "about 77% . . .". At the June 1991 meeting in Nashville, BSD Networking Release 2 was available.

Net2, a USA-Russia collaboration, was turned into a commercial product, BSDi. (It had been complete in 1991, but it was only released in 1993 thanks to legal delays introduced by UNIX System Laboratories, which filed suit to the effect that BSDi infringed USL's copyright, and sought an injunction to prevent sales.)

On March 3, 1993, the court denied the preliminary injunction. On March 30, 1993, Judge Dickinson Debevoise of the US District Court of New Jersey reaffirmed his denial of USL's motion.

USL filed a motion for reconsideration. The court denied the motion. In June 1993, the Regents of the University of California struck back, filing suit against USL.

In the meantime, Novell had acquired USL.

On Friday, February 4, 1994, Novell and the University of California agreed to drop all suits and countersuits.

BSDi immediately announced the availability of 4.4-Lite.

Could someone bring this to the attention of Darl McBride?