Network Intrusion Detection: Book Review

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

New Riders Publishing sent me some books for review recently. I like this publisher’s list of security titles, and I enjoy being an occasional technical reviewer on contract for them (there: that takes care of disclosing a possible conflict of interest as I write this review). _Network Intrusion Detection: An Analyst’s Handbook, Second Edition_ by Stephen Northcutt, Judy Novak and Donald McLachlan strikes me a superb instruction manual for everyone concerned with intrusion detection and analysis – which is to say, everyone who runs a network connected to the Internet.

The book opens with 32 pages of roman-numeral-numbered material. Ho-hum, who cares? Well in this case, the introduction includes a thoroughly fascinating introduction with a history of the “Shadow” program used to analyze TCP/IP traffic; an overview of threats to security; a cogent summary of lessons learned from the Y2K experience; a review of distributed denial-of-service (DDoS) attacks; a stimulating analysis of “macro threats” (global and economic influences on information security); and an intelligent analysis of what the authors call “micro threats” (the devil in the details of running information systems). And all that is just the beginning.

* Chapter 1, “IP Concepts” introduces (or reviews) the basic concepts and terminology of the Transmission Control Protocol/Internet Protocol (TCP/IP). As the authors note, the chapter is useful even for experts because it can provide good diagrams and explanations useful in teaching beginners.

* Chapter 2, “Introduction to TCPdump and . . . TCP” presents a tutorial on how to use TCPdump or Windump programs to analyze packets.

* Chapter 3 discusses fragmentation of packets to avoid some intrusion detection systems (IDSs) and filters.

* Chapter 4 introduces the Internet Control Message Protocol (ICMP) and a series of mapping techniques used by intruders scoping out their potential victims. It also discusses several ICMP-based DDoS attack techniques and other malicious misuses of ICMP.

* Chapter 5 discusses normal stimulus-response sequences and some of the “protocol benders” implemented by malicious hackers.

The book continues to a total of 22 chapters, each a jewel of methodical, concise, interesting writing with plenty of examples and exercises for the serious student. I particularly like the inclusion of in-chapter partial summaries that help a reader understand where they are heading in the rest of the chapter.
The authors write with assurance and grace, and they have a noticeable sense of humor. The text is enlivened by personal experiences and by its practical orientation. It is never dull.

The only oddity I noticed is that on my copy, at least, the name of the third author, Donald McLachlan appeared on the flyleaf (page iii) but, strangely, not on the cover itself. Perhaps it was a printing error.

Readers must understand that I am not a technical expert in intrusion detection, but it is a foundation element of modern information security and I have been following developments in this area for many years. With that warning in mind, I do unhesitatingly recommend this book to readers and suggest it as a candidate to colleagues considering textbooks for university upper-level and graduate courses in intrusion detection. My congratulations and thanks to the authors, editors and publishers of this work.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.