RIK FARROW

book reviews

I guess I get a lot of books for review because I began writing articles about UNIX and security back in 1986. I get more books than I can read, as well as some I don't think I would ever read—ones whose topics are far afield from what I really need to know about.

Recently, I received several books all with related topics, and thought that they deserved special treatment. Two of the books are about using Snort, while the third does mention Snort and IDS but represents a much deeper topic: network security monitoring.

MANAGING SECURITY WITH SNORT AND IDS TOOLS

Kerry Cox and Christopher Gerg

Sebastopol, CA: O'Reilly and Associates, 2004. Pp. 269.
ISBN 0-596-00661-6.

SNORT 2.1 INTRUSION DETECTION, 2D ED.

Jay Beale et al.

Rockland, MA: Syngress Publishing Inc., 2004. Pp. 716.
ISBN 1-931836-04-3.

Jay Beale is the editor of the *Snort 2.1* book, as there are actually many authors. The cast of characters involved in *Snort 2.1* is both an advantage and a disadvantage. On the plus side, you get chapters written by Snort developers. On the minus side, you get a book that could be better organized and that still contains some mistakes and typos which also plagued the first edition.

Managing Security with Snort is shorter and written by Snort users rather than developers and users. Being an O'Reilly book, it is formatted differently and, as a result, is better organized than the Syngress book. I found the instructions for building and using Snort, or a Snort-related tool like ACID, clear and easy to follow (ACID has been and still is a bear to build).

There are certainly differences deeper than formatting between these books. While either will get you going with Snort, *Snort 2.1*, with its greater length, does get into more details. For example, *Managing Security* has five pages on configuring and using Barnyard, a tool for processing Snort alerts asynchronously. *Snort 2.1* devotes an entire chapter, 75 pages, to working with Barnyard.

I had wondered how these books would handle Snort rule writing. The two deal with this topic in almost the same manner. Each book explains the parts of Snort rules and provides a couple of examples, but neither one has a tutorial. I consider rule writing/editing a critical topic in a rule-based IDS tool, and was disappointed that neither book goes deeply enough into this area. *Managing Security* actually misses an important new set of rule options, `flow`, which allows rules to include the distinction of a packet going to a client or a server.

I can recommend either of these books, and suggest that you make your decision based on how deeply you want to go into Snort and related tools.

THE TAO OF NETWORK SECURITY MONITORING

Richard Bejtlich

Boston: Addison-Wesley, 2004. Pp. 798.
ISBN 0-321-24677-2.

Bejtlich honed his network monitoring skills working for the Air Force Computer Emergency Response Team, and his experience shows. Instead of talking about preventing intrusions, Bejtlich assumes there will be intrusions. His approach involves collecting as much network data as possible, so this information can be used to determine what has happened on your network in the past. The data includes IDS alerts, flow data, and complete packet dumps.

Bejtlich successfully explains why IDS alerts are not enough. He demonstrates how having both flows and packet data helps analysts determine when an alert represents a successful attack. Bejtlich does briefly mention Snort, but he covers many other tools as well. Bejtlich is particularly fond of Sguil, a tool for querying back-end databases that contain the mountain of alerts, flows, and packets generated in his approach.

Bejtlich presents network and system management (NSM) as a philosophy, backed with lots of practical advice from someone who uses NSM in real life. I highly recommend this book if you are serious about your network security and want to go beyond viewing IDS alerts.