



Incident Response

By Kenneth R. van Wyk & Richard Forno

O'Reilly Press, \$34.95 (retail)

ISBN # 0-59600-130-4

Reviewed by Warren Volz

With the ever-increasing number of security vulnerabilities on the Internet it is a great time to learn about how to handle a network security incident if one occurs. Incident Response is a book with a little for technical people and a little for business people. The book provides a good overview of setting up a team and/or procedure for handling an incident. It outlines

what an incident is and how to deal with an incident. The book also covers different organizational structures that could be used to set up an incident response team.

The book is broken up into 4 major categories:

- What an incident response is
- Building incident response teams, planning incident response programs
- What to do when an incident happens and what tools to use
- Resources and sample incident reports.

The beginning of this book gives a good overview of what an incident is and gives a good overview of incident response teams. I think the authors do a good job of laying out the details needed to form an effective team and create a response plan. I especially like the overview of the different types of attacks and background that the authors give in chapter 5. Other things that I found useful were the sample incident reports that were provided, the list of FIRST (Forum of Incident Response and Security Teams), and the Tools of the Trade resource listing.

Overall I would give this book a must read rating for any person that has questions about what an incident is and how to deal with it. I would also recommend this book to anyone that needs a book to suggest his/her boss read to prove that you need a more effective way to deal with security concerns. I personally would have liked to see more technical coverage in the book, but I think it reaches the target audience very effectively.

Rating: Three out of Five stars