[PDF] Network Intrusion Detection: An Analysts' Handbook

Stephen Northcutt - pdf download free book

Books Details:
Title: Network Intrusion Detection:
Author: Stephen Northcutt
Released: 1999-08-15
Language:
Pages: 267
ISBN: 0735708681
ISBN13: 978-0735708686
ASIN: 0735708681

---

pdf, mobi, epub, azw, kindle

Description:

Network Intrusion Detection: An Analyst's Handbook explains some of what you need to know to prevent unauthorized accesses of your networked computers and minimize the damage intruders can do. It emphasizes, though, proven techniques for recognizing attacks while they're underway. Without placing too much emphasis (or blame, for that matter) on any operating system or other software product, author Stephen Northcutt explains ways to spot suspicious behavior and deal with it, both automatically and manually.

The case studies, large and small, are the best part of this book. Northcutt opens with a technical brief on the methods used by Kevin Mitnick in his attack upon Tsutomu Shimomura's server. In

documenting that famous attack, Northcutt explains SYN flooding and TCP hijacking with clarity and detail: readers get a precise picture of what Mitnick did and how Shimomura's machine reacted. A former security expert for the U.S. Department of Defense, Northcutt explains how a system administrator would detect and defeat an attack like Mitnick's. Another case study appears later in the book, this one in the form of a line-by-line analysis of a .history file that shows how a bad guy with root privileges attacked a Domain Name System (DNS) server. Reading Northcutt's analysis is like reading a play-by-play account of a football match. *Network Intrusion Detection* is one of the most readable technical books around. *--David Wall*

Topics covered: Catching intruders in the act by recognizing the characteristics of various kinds of attacks in real time, both manually and with the use of filters and other automated systems; techniques for identifying security weaknesses and minimizing false security alarms.

From the Inside Flap "The 2nd Edition of Network Intrusion Detection fortifies its position as the primary manual for front-line intrusion detectors. One of this book's major achievements is that it succinctly and thoroughly addresses the training needs of personnel operating sophisticated Intrusion Detection Systems. No other published volume gives hands-on analysts the tools to separate false positives from true alerts on a daily basis.

Buy this book if your job involves intrusion detection, incident response, or computer security in general. You will walk away wiser and better prepared to face the wiles of the Internet, and your company will benefit from an improved security posture."

-Captain Richard Bejtlich, Intrusion Technician, Air Force Computer Emergency Response Team

"This is the ONLY book addressing effective network intrusion detection and response. The content comes directly from daily "front-line" experience, and the material represents the best consensus from a variety of expert practitioners. There is not a resource out there which has more relevant than this book. I am rewriting my filters today based on what I have read." -Andy Johnston, Distributed System Manager, Office of Information Technology, University of Maryland, Baltimore County

"I love the writing style. Conversational with just enough humor to keep it interesting. Points like "seasoned administrators can skip this chapter" and "this point is important to understanding the rest of the chapter" are great guides to helping the reader work their way through the material."

-Chris Brenton, Senior Research Engineer at Dartmouth's Institute for Security Technology Studies

"I was particularly impressed by the suggested presentations to managers for laying out a cost-benefit analysis of the overall benefits of purchasing a host-based intrusion detection system and appropriate training for analysts. Intrusion Detection Systems can be extremely costly and may seem like "money pits" to people who do not understand the need for monitoring networks. This book would be extremely useful for anyone wishing to approach corporate managers on both of these issues."

-John Furlong, Security Consultant --This text refers to an out of print or unavailable edition of this title.

- Title: Network Intrusion Detection: An Analysts' Handbook
- Author: Stephen Northcutt
- Released: 1999-08-15
- Language:
- Pages: 267
- ISBN: 0735708681
- ISBN13: 978-0735708686
- ASIN: 0735708681