[PDF] Network Intrusion Detection: An Analyst's Handbook (2nd Edition)

Stephen Northcutt, Judy Novak, Donald McLachlan - pdf download free book

---

Books Details:
Title: Network Intrusion Detection:
Author: Stephen Northcutt, Judy Nova
Released: 2000-09-22
Language:
Pages: 450
ISBN: 0735710082
ISBN13: 978-0735710085
ASIN: 0735710082

---

pdf, mobi, epub, azw, kindle

Description:

A collection of after-action reports on a variety of network attacks, *Network Intrusion Detection* enables you to learn from others' mistakes as you endeavor to protect your networks from intrusion. Authors Stephen Northcutt and Judy Novak document real attacks on systems, and highlight characteristics that you--you being a network communications analyst or security specialist--can look for on your own machines. The authors mince no words, and advise you on the detection tools to use (they like and use Snort, as well as Shadow, Tripwire, TCP Wrappers, and others) and how to use them. This second edition of the book includes less about year-2000 preparation and more about the latest in attacks, countermeasures, and the growing community of white-hat hackers who share

information to keep systems safe.

In teaching their readers about the attacks that exploit a particular protocol or service, the authors typically present a TCPdump listing that shows an attack, and then comment upon it. They tell you what the attackers did, how successful they were, and how the attack might have been detected and shut down. To cite one example, there's a very detailed analysis of Kevin Mitnick's famous attack (a SYN flood, combined with TCP hijacking) on one of Tsutomu Shimomura's machines. By following the advice in this book, you'll likely do well in protecting your machines against people whom the authors call "script kiddies" --small-time hackers who follow published recipes (or run prewritten routines). Also, you'll be about as prepared as you can be against more skilled attackers who make up their attacks on their own. This is great reading for anyone who's involved in developing filters to ward off attacks or monitoring network communications for suspicious activity. It's also a valuable resource for someone who's evaluating network countermeasures in preparation for deployment. -- *David Wall*

Topics covered: Analysis of TCP/IP traffic, with an eye toward detecting and halting malicious activity, both manually and automatically. Subjects include tools for finding weaknesses and initiating attacks, and the signatures that identify these tools. There's discussion of the vulnerabilities that exist in services, such as IMAP and Domain Name System (DNS).

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

- Title: Network Intrusion Detection: An Analyst's Handbook (2nd Edition)
- Author: Stephen Northcutt, Judy Novak, Donald McLachlan
- Released: 2000-09-22
- Language:
- Pages: 450
- ISBN: 0735710082
- ISBN13: 978-0735710085
- ASIN: 0735710082
