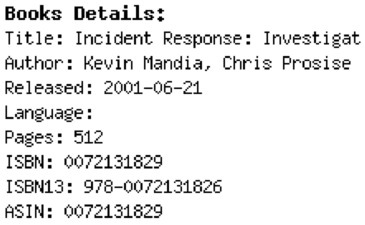
[PDF] Incident Response: Investigating Computer Crime

Kevin Mandia, Chris Prosise - pdf download free book



Books Details:
Title: Incident Response: Investigat
Author: Kevin Mandia, Chris Prosise
Released: 2001-06-21
Language:
Pages: 512
ISBN: 0072131829
ISBN13: 978-0072131826
ASIN: 0072131829

pdf, mobi, epub, azw, kindle

Description:

A strong system of defenses will save your systems from falling victim to published and otherwise uninventive attacks, but even the most heavily defended system can be cracked under the right conditions. *Incident Response* aims to teach you how to determine when an attack has occurred or is underway--they're often hard to spot--and show you what to do about it. Authors Kevin Mandia and Chris Prosise favor a tools- and procedures-centric approach to the subject, thereby distinguishing this book from others that catalog particular attacks and methods for dealing with each one. The approach is more generic, and therefore better suited to dealing with newly emerging attack techniques.

Anti-attack procedures are presented with the goal of identifying, apprehending, and successfully prosecuting attackers. The advice on carefully preserving volatile information, such as the list of processes active at the time of an attack, is easy to follow. The book is quick to endorse tools, the functionalities of which are described so as to inspire creative applications. Information on bad-guy behavior is top quality as well, giving readers knowledge of how to interpret logs and other observed phenomena. Mandia and Prosise don't--and can't--offer a foolproof guide to catching crackers in the act, but they do offer a great "best practices" guide to active surveillance. *--David Wall*

Topics covered: Monitoring computer systems for evidence of malicious activity, and reacting to such activity when it's detected. With coverage of Windows and Unix systems as well as non-platform-specific resources like Web services and routers, the book covers the fundamentals of incident response, processes for gathering evidence of an attack, and tools for making forensic work easier.

Review "... poorly trained network administrators and the lack of firewalls and intrustion detection systems still make it difficult to find the source and strategy of the attack." Computerworld article (8/21/00) on Incident Response featuring David Dittrich, a researcher who spoke at the Usenix Security Symposium."

- Title: Incident Response: Investigating Computer Crime
- Author: Kevin Mandia, Chris Prosise
- Released: 2001-06-21
- Language:
- Pages: 512
- ISBN: 0072131829
- ISBN13: 978-0072131826
- ASIN: 0072131829
