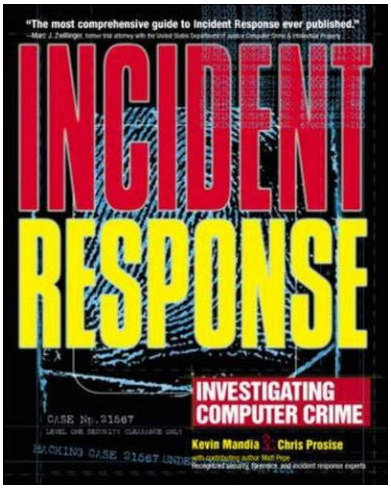
[PDF] Incident Response: Investigating Computer Crime

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

Only RUB 193.34/month. Incident Response and Computer Crime Investigations. STUDY. Flashcards.Â 1. Prevention, detection, and response of an attack is the primary goal. 2. Not a matter of if but when.Â A strategy to investigate a new path based on the evidence found. Which can expand the scope of the investigation. What is data reduction? Investigating Computer- Related Crime a Handbook for Corporate Investigators. Read more. Agatha Christie: Investigating Femininity (Crime Files). Read more. Computer Forensics: Computer Crime Scene Investigation. Read more. Computer Forensics: Investigating Network Intrusions and Cybercrime.Â Computer Incident Response and Product Security Damir Rajnovic Cisco Press 8 0 0 East 96th Street Indianapolis, IN 4 6 Incident Response and Computer Forensics, 2nd Edition. INCIDENT RESPONSE & COMPUTER FORENSICS, SECOND EDITION This page intentionally left blank. Incident response & comp The Effective Incident Response Team. Computer Incident Response and Product Security (Networking Technology: Security). Cybercrime is a crime that involves a computer and a network.[1][2] The computer may have been used in the commission of a crime, or it may be the target.[3] Cybercrime may harm someone's security and financial health.[4]. There are many privacy concerns surrounding Cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise.Â Classifications[edit]. With traditional crime reducing, global communities continue to witness a sporadic growth in cybercrime.[12] Computer crime encompasses a broad range of activities.[13]. Financial fraud crimes[edit]. Main article: Internet fraud. Incident response is a multidisciplinary science that resolves computer crime and complex legal issues, chronological methodologies and technical computer techniques. The commercial industry has embraced and adopted technology that detects hacker incidents. Companies are swamped with real attacks, yet very few have any methodology or knowledge to resolve these attacks. "Incident Response: Investigating Computer Crime" will be the only book on the market that provides the information on incident response that network professionals need to conquer attacks. xiv Incident Response & Computer Forensics. Creating an In-Depth Response Toolkit . . . Collecting Live Response Data . . .Â We describe real-life incidents we investigated and give you the inside information on how they were solved. xxviii Incident Response & Computer Forensics. We set up the scene of a crime by providing a detailed description of scenarios as if they are actually happening to you. This is different from the â€œWhat Can Happenâ€ element because it provides a scenario in much more detail.