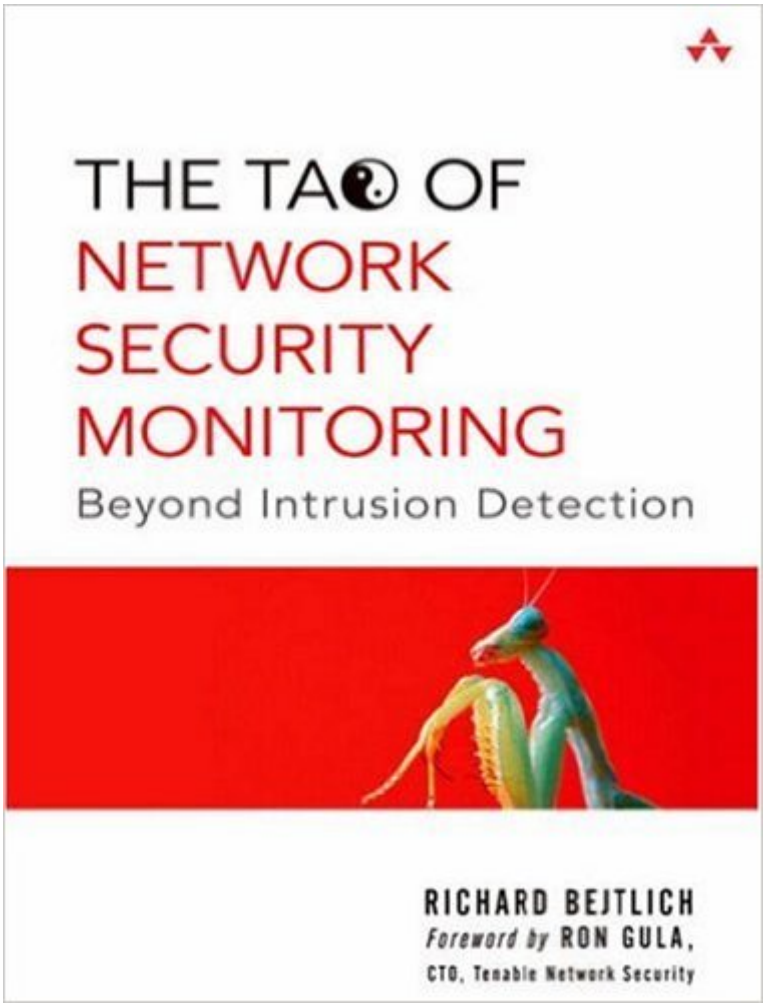
The Tao Of Network Security Monitoring: Beyond Intrusion Detection



Synopsis

"The book you are about to read will arm you with the knowledge you need to defend your network from attackersâ ”both the obvious and the not so obvious.... If you are new to network security, don't put this book back on the shelf! This is a great book for beginners and I wish I had access to it many years ago. If you've learned the basics of TCP/IP protocols and run an open source or commercial IDS, you may be asking 'What's next?' If so, this book is for you." Â Â Â Â Â Â Â Â Â Â â ”Ron Gula, founder and CTO, Tenable Network Security, from the Foreword "Richard Bejtlich has a good perspective on Internet securityâ ”one that is orderly and practical at the same time. He keeps readers grounded and addresses the fundamentals in an accessible way." Â Â Â Â Â Â Â Â Â Â â ”Marcus Ranum, TruSecure "This book is not about security or network monitoring: It's about both, and in reality these are two aspects of the same problem. You can easily find people who are security experts or network monitors, but this book explains how to master both topics." Â Â Â Â Â Â Â Â Â Â â ”Luca Deri, ntop.org "This book will enable security professionals of all skill sets to improve their understanding of what it takes to set up, maintain, and utilize a successful network intrusion detection strategy."Â Â Â Â Â Â Â Â Â Â â ”Kirby Kuehl, Cisco Systems Every network can be compromised. There are too many systems, offering too many services, running too many flawed applications. No amount of careful coding, patch management, or access control can keep out every attacker. If prevention eventually fails, how do you prepare for the intrusions that will eventually happen? Network security monitoring (NSM) equips security staff to deal with the inevitable consequences of too few resources and too many responsibilities. NSM collects the data needed to generate better assessment, detection, and response processesâ ”resulting in decreased impact from unauthorized activities. In The Tao of Network Security Monitoring , Richard Bejtlich explores the products, people, and processes that implement the NSM model. By focusing on case studies and the application of open source tools, he helps you gain hands-on knowledge of how to better defend networks and how to mitigate damage from security incidents. Inside, you will find in-depth information on the following areas. The NSM operational framework and deployment considerations. How to use a variety of open-source toolsâ ”including Sguil, Argus, and Etherealâ ”to mine network traffic for full content, session, statistical, and alert data. Best practices for conducting emergency NSM in an incident response scenario, evaluating monitoring vendors, and deploying an NSM architecture. Developing and applying knowledge of weapons, tactics, telecommunications, system administration, scripting, and programming for NSM. The best tools for generating arbitrary packets, exploiting flaws, manipulating traffic, and conducting reconnaissance.

Whether you are new to network intrusion detection and incident response, or a computer-security veteran, this book will enable you to quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging threats.

Book Information

Paperback: 832 pages

Publisher: Addison-Wesley Professional; 1 edition (July 22, 2004)

Language: English

ISBN-10: 0321246772

ISBN-13: 978-0321246776

Product Dimensions: 7 x 1.8 x 8.8 inches

Shipping Weight: 2.6 pounds (View shipping rates and policies)

Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (31 customer reviews)

Best Sellers Rank: #103,991 in Books (See Top 100 in Books) #24 inÂ Books > Computers & Technology > Certification > CompTIA #51 inÂ Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks #83 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

Here is a really cool security book, that made me lose half a nigh sleep when I first got it. Richard Bejtlich "Tao of Network Security Monitoring" ("Tao of NSM") covers the process, tools and analysis techniques for monitoring your network using intrusion detection, session data, traffic statistical information and other data. Here are some of the book highlights. The book starts from a really exciting and fun background on security, risk and the need to monitor networks and systems. Topics such as the classic "threat x vulnerability x value = risk" formula to threat modeling and limitation of attack prevention technologies are included. A nice thing on the process side is the "assess -> protect -> detect -> respond" loop, that defines a security process for an organization on a high level. Threat analysis material seems to have military origin, but is enlightening for other types of organizations as well. NSM is introduced as being ’beyond IDS’ with some coverage on why IDS deployments fail and what else is needed (NSM process and tools, that is). A great and rarely appreciated idea expressed in the book is that the intruders are often smarter than defenders. It presents a stark contrast to all this "staying ahead of the hackers", which makes no sense in many cases as the attackers are in fact far ahead. NSM approach will indeed work against the advanced attackers, albeit a high resource cost to the defending organization. Such ’worst case’ scenario

preparations are extremely rare in other security books. Detecting such intruder is covered during their five phases of compromise (from reconnaissance to using/abusing the system).

Richard Bejtlich hits one out of the park with this terrific book. In one stroke, he moves the art and science of intrusion detection out of the little leagues and into the majors. If you've already run through articles and books with advice like "just load SNORT and start tuning", this book will shift you to an all-star level in which thousands of machines across enterprise networks can be monitored and protected.Network security monitoring (NSM) is the discipline of collecting and interpreting detailed network traffic to find and foil attackers. Although it may seem like Intrusion Detection (and IDSs), the relationship between IDSs and NSM is like that between Bonzo the chimp and King Kong. Almost anybody could handle a chimp for a few hours - or you'd think so from watching the movies - but bringing King Kong into your neighborhood means you really have to know what you're doing. He'll take a lot of feeding and special care. On the other hand, he does much more than Bonzo can to protect your assets. Network security monitoring is the King Kong of intrusion detection techniques.The author presents detailed information on a large variety of network traffic capture and analysis tools, techniques, and topologies. Nearly all are public domain and open source. The few exceptions are tools specialized for industry-dominating Cisco and its proprietary formats and protocols. A few hours on the Internet with this book in hand can give you just about all the tools needed to follow his examples and to build your own network security monitoring environment.Basic network activity capture is addressed through packages like the fundamental libpcap libraries, and the tools Tcpdump, Tethereal, Ethereal, and Snort (in its packet-capture mode).

This is a great book. With most geek books, I browse and grab what I need. With this one, I even read the apendices!At first, the author's tone put me off. He spends the introductory chapters talking about the "Way" of Network Security Monitoring, (capitalized) and how it's much better than other approaches. It felt a little like, "My Burping Crane Kung-Fu will defeat your Shining Fist techniques!" I really didn't see much difference between what he was talking about and other approaches. I admit to being much newer to this discipline than the author, and he has an impressive appendix on the intellectual history of intrusion detection (uncapitalized). So it may be that the lessons he advocates have already been internalized; my exposure may have been to a field that has already moved up to his standard. But I have a hard time imagining that intrusion analysts have ever been satisfied with a single approach with no correlation. As I understand what he means by upper-case NSM, it's

basically the efficient use of multiple techniques to detect intrusions. I can’t see trying to argue the contrary position.Ah, but then we get to the good stuff. He goes through the major types of indicators and the means of reviewing them. He covers the use of a number of important tools, but doesn’t rehash what is better covered elsewhere. For example, he doesn’t bother covering Snort, because there are plenty of books on Snort already. If you are reading the book, it’s almost a certainty that you are familiar with Snort. Good call to skip over that. Instead, he covers some other tools that might be useful in the same area. He also refers to tons of other books. I made a lengthy wish-list based on his recommendations and they’ve been good.

Dmca