The Tao of Network Security Monitoring: Beyond Intrusion Detection

Richard Bejtlich

The Tao of Network Security Monitoring: Beyond Intrusion Detection

Richard Bejtlich

The Tao of Network Security Monitoring: Beyond Intrusion Detection Richard Bejtlich

"The book you are about to read will arm you with the knowledge you need to defend your network from attackers—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."

—Ron Gula, founder and CTO, Tenable Network Security, from the Foreword

"Richard Bejtlich has a good perspective on Internet security—one that is orderly and practical at the same time. He keeps readers grounded and addresses the fundamentals in an accessible way."

—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."

—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."

—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 processes—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 tools—including Sguil, Argus, and Ethereal—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.

Download and Read Free Online The Tao of Network Security Monitoring: Beyond Intrusion Detection Richard Bejtlich

---

From reader reviews:

Louise Wax:

Book is definitely written, printed, or highlighted for everything. You can learn everything you want by a publication. Book has a different type. As it is known to us that book is important matter to bring us around the world. Beside that you can your reading proficiency was fluently. A reserve The Tao of Network Security Monitoring: Beyond Intrusion Detection will make you to become smarter. You can feel considerably more confidence if you can know about everything. But some of you think that will open or reading a new book make you bored. It is far from make you fun. Why they may be thought like that? Have you searching for best book or suitable book with you?

John Honeycutt:

Playing with family in the park, coming to see the coastal world or hanging out with close friends is thing that usually you have done when you have spare time, in that case why you don't try factor that really opposite from that. One particular activity that make you not feeling tired but still relaxing, trilling like on roller coaster you already been ride on and with addition of knowledge. Even you love The Tao of Network Security Monitoring: Beyond Intrusion Detection, you may enjoy both. It is very good combination right, you still would like to miss it? What kind of hang type is it? Oh seriously its mind hangout men. What? Still don't obtain it, oh come on its referred to as reading friends.

Dan Fry:

Can you one of the book lovers? If so, do you ever feeling doubt when you are in the book store? Try to pick one book that you never know the inside because don't evaluate book by its handle may doesn't work here is difficult job because you are frightened that the inside maybe not while fantastic as in the outside search likes. Maybe you answer is usually The Tao of Network Security Monitoring: Beyond Intrusion Detection why because the amazing cover that make you consider in regards to the content will not disappoint anyone. The inside or content is fantastic as the outside or cover. Your reading sixth sense will directly assist you to pick up this book.

Paul Jackson:

Many people spending their time by playing outside together with friends, fun activity with family or just watching TV the whole day. You can have new activity to spend your whole day by reading through a book. Ugh, think reading a book can actually hard because you have to accept the book everywhere? It alright you can have the e-book, getting everywhere you want in your Cell phone. Like The Tao of Network Security Monitoring: Beyond Intrusion Detection which is keeping the e-book version. So , why not try out this book? Let's observe.

Read The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich for online ebook

The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich books to read online.

Online The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich ebook PDF download

The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich Doc

The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich Mobipocket

The Tao of Network Security Monitoring: Beyond Intrusion Detection by Richard Bejtlich EPub