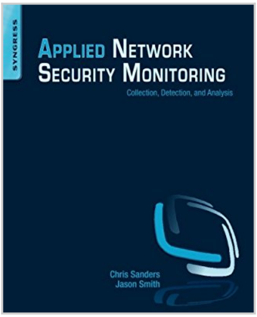
SYNGRESS
Applied Network Security Monitoring
Collection, Detection, and Analysis
Chris Sanders
Jason Smith

Applied Network Security Monitoring: Collection, Detection, and Analysis

By Chris Sanders, Jason Smith

Applied Network Security Monitoring: Collection, Detection, and Analysis
By Chris Sanders, Jason Smith

Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach, complete with real-world examples that teach you the key concepts of NSM.

Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, your ability to detect and respond to that intrusion can be the difference between a small incident and a major disaster.

The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical knowledge that you can apply immediately.

- Discusses the proper methods for planning and executing an NSM data collection strategy
- Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, PRADS, and more
- The first book to define multiple analysis frameworks that can be used for performing NSM investigations in a structured and systematic manner
- Loaded with practical examples that make use of the Security Onion Linux distribution
- Companion website includes up-to-date blogs from the authors about the latest developments in NSM, complete with supplementary book materials

If you've never performed NSM analysis, *Applied Network Security Monitoring* will help you grasp the core concepts needed to become an effective analyst. If you are already working in an analysis role, this book will allow you to refine your analytic technique and increase your effectiveness.

You will get caught off guard, you will be blind sided, and sometimes you will lose the fight to prevent attackers from accessing your network. This book is about equipping you with the right tools for collecting the data you need, detecting malicious activity, and performing the analysis that will help you understand the nature of an intrusion. Although prevention can eventually fail, NSM doesn't have to.

** Note: All author royalties from the sale of Applied NSM are being donated to a number of charities selected by the authors.

Applied Network Security Monitoring: Collection, Detection, and Analysis

By Chris Sanders, Jason Smith

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith

Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach, complete with real-world examples that teach you the key concepts of NSM.

Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, your ability to detect and respond to that intrusion can be the difference between a small incident and a major disaster.

The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical knowledge that you can apply immediately.

- Discusses the proper methods for planning and executing an NSM data collection strategy
- Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, PRADS, and more
- The first book to define multiple analysis frameworks that can be used for performing NSM investigations in a structured and systematic manner
- Loaded with practical examples that make use of the Security Onion Linux distribution
- Companion website includes up-to-date blogs from the authors about the latest developments in NSM, complete with supplementary book materials

If you've never performed NSM analysis, *Applied Network Security Monitoring* will help you grasp the core concepts needed to become an effective analyst. If you are already working in an analysis role, this book will allow you to refine your analytic technique and increase your effectiveness.

You will get caught off guard, you will be blind sided, and sometimes you will lose the fight to prevent attackers from accessing your network. This book is about equipping you with the right tools for collecting the data you need, detecting malicious activity, and performing the analysis that will help you understand the nature of an intrusion. Although prevention can eventually fail, NSM doesn't have to.

** Note: All author royalties from the sale of Applied NSM are being donated to a number of charities selected by the authors.

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith Bibliography

- Sales Rank: #187376 in Books

- Published on: 2013-12-19
- Released on: 2013-12-05
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x 1.12" w x 7.50" l, 2.20 pounds
- Binding: Paperback
- 496 pages

Editorial Review

Review

"... an extremely informative dive into the realm of network security data collection and analysis...well organized and thought through...I have only positive comments from my study." ***-The Ethical Hacker Network*, Oct 31, 2014**

About the Author
Chris Sanders is an information security consultant, author, and researcher originally from Mayfield, Kentucky. That's thirty miles southwest of a little town called Possum Trot, forty miles southeast of a hole in the wall named Monkey's Eyebrow, and just north of a bend in the road that really is named Podunk.

Chris is a Senior Security Analyst with InGuardians. He has as extensive experience supporting multiple government and military agencies, as well as several Fortune 500 companies. In multiple roles with the US Department of Defense, Chris significantly helped to further to role of the Computer Network Defense Service Provider (CNDSP) model, and helped to create several NSM and intelligence tools currently being used to defend the interests of the nation.

Chris has authored several books and articles, including the international best seller "Practical Packet Analysis" form No Starch Press, currently in its second edition. Chris currently holds several industry certifications, including the SANS GSE and CISSP distinctions.

In 2008, Chris founded the Rural Technology Fund. The RTF is a 501(c)(3) non-profit organization designed to provide scholarship opportunities to students form rural areas pursuing careers in computer technology. The organization also promotes technology advocacy in rural areas through various support programs. The RTF has provided thousands of dollars in scholarships and support to rural students.

When Chris isn't buried knee-deep in packets, he enjoys watching University of Kentucky Wildcat basketball, being a BBQ Pitmaster, amateur drone building, and spending time at the beach. Chris currently resides in Charleston, South Carolina with his wife Ellen.

Chris blogs at appliednsm.com and chrissanders.org. He is on Twitter as @chrissanders88.

Users Review

From reader reviews:

Karen Chan:

Book is actually written, printed, or created for everything. You can learn everything you want by a book. Book has a different type. To be sure that book is important point to bring us around the world. Close to that you can your reading expertise was fluently. A reserve Applied Network Security Monitoring: Collection, Detection, and Analysis will make you to always be smarter. You can feel far more confidence if you can know about almost everything. But some of you think this open or reading the book make you bored. It is not necessarily make you fun. Why they might be thought like that? Have you searching for best book or acceptable book with you?

Henry Knight:

What do you ponder on book? It is just for students since they're still students or the item for all people in the world, the particular best subject for that? Just you can be answered for that concern above. Every person has various personality and hobby per other. Don't to be pressured someone or something that they don't need do that. You must know how great in addition to important the book Applied Network Security Monitoring: Collection, Detection, and Analysis. All type of book is it possible to see on many methods. You can look for the internet solutions or other social media.

Suk Barry:

Book is to be different for each grade. Book for children till adult are different content. To be sure that book is very important for people. The book Applied Network Security Monitoring: Collection, Detection, and Analysis was making you to know about other understanding and of course you can take more information. It is quite advantages for you. The publication Applied Network Security Monitoring: Collection, Detection, and Analysis is not only giving you a lot more new information but also to be your friend when you sense bored. You can spend your current spend time to read your guide. Try to make relationship with the book Applied Network Security Monitoring: Collection, Detection, and Analysis. You never sense lose out for everything in the event you read some books.

Leah Humphries:

This book untitled Applied Network Security Monitoring: Collection, Detection, and Analysis to be one of several books that will best seller in this year, here is because when you read this publication you can get a lot of benefit on it. You will easily to buy this book in the book retail store or you can order it by using online. The publisher in this book sells the e-book too. It makes you easier to read this book, as you can read this book in your Smartphone. So there is no reason to you to past this reserve from your list.

Download and Read Online Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith #HVQ24OB01ZW

Read Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith for online ebook

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith 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 Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith books to read online.

Online Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith ebook PDF download

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith Doc

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith Mobipocket

Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith EPub

HVQ24OB01ZW: Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith