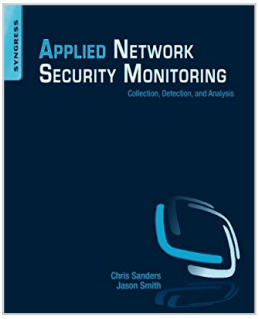

Applied Network Security Monitoring: Collection, Detection, and Analysis

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:

Velma Stuart:

What do you concerning book? It is not important to you? Or just adding material when you need something to explain what your own problem? How about your free time? Or are you busy man or woman? If you don't have spare time to try and do others business, it is give you a sense of feeling bored faster. And you have extra time? What did you do? All people has many questions above. They have to answer that question since just their can do this. It said that about guide. Book is familiar on every person. Yes, it is right. Because start from on pre-school until university need this kind of Applied Network Security Monitoring: Collection,

Detection, and Analysis to read.

Omar Carter:

In this 21st century, people become competitive in every single way. By being competitive now, people have do something to make these people survives, being in the middle of the crowded place and notice by simply surrounding. One thing that oftentimes many people have underestimated it for a while is reading. Yeah, by reading a e-book your ability to survive increase then having chance to endure than other is high. For you personally who want to start reading any book, we give you that Applied Network Security Monitoring: Collection, Detection, and Analysis book as nice and daily reading book. Why, because this book is more than just a book.

Jeffrey Bumgardner:

In this era which is the greater individual or who has ability in doing something more are more treasured than other. Do you want to become one among it? It is just simple method to have that. What you must do is just spending your time not very much but quite enough to get a look at some books. Among the books in the top checklist in your reading list will be Applied Network Security Monitoring: Collection, Detection, and Analysis. This book that is certainly qualified as The Hungry Hillsides can get you closer in turning out to be precious person. By looking upwards and review this book you can get many advantages.

Concepcion Shaw:

What is your hobby? Have you heard that will question when you got students? We believe that that problem was given by teacher to their students. Many kinds of hobby, All people has different hobby. And you also know that little person like reading or as reading become their hobby. You should know that reading is very important in addition to book as to be the thing. Book is important thing to provide you knowledge, except your own personal teacher or lecturer. You discover good news or update regarding something by book. Numerous books that can you decide to try be your object. One of them is Applied Network Security Monitoring: Collection, Detection, and Analysis.

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

W0B3M9XL5DO: Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith