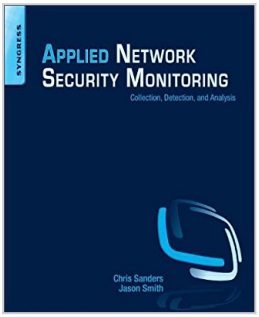

Applied Network Security Monitoring: Collection, Detection, and Analysis

By Chris Sanders, Jason Smith

Download now

Read Online

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 to NSM, complete with dozens of 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, it is your ability to detect and respond to that intrusion that 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 scenarios complete with sample data.

If you've never performed NSM analysis, *Applied Network Security Monitoring* will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job.

- Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst
- Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus
- Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples
- Companion website includes up-to-date blogs from the authors about the latest developments in NSM

Download Applied Network Security Monitoring: Collection, D ...pdf

Read Online Applied Network Security Monitoring: Collection, ...pdf

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 to NSM, complete with dozens of 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, it is your ability to detect and respond to that intrusion that 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 scenarios complete with sample data.

If you've never performed NSM analysis, *Applied Network Security Monitoring* will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job.

- Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst
- Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus
- Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples
- Companion website includes up-to-date blogs from the authors about the latest developments in NSM

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

- Sales Rank: #131499 in eBooks
- Published on: 2013-11-26
- Released on: 2013-11-26
- Format: Kindle eBook

Download Applied Network Security Monitoring: Collection, D ...pdf

Read Online Applied Network Security Monitoring: Collection, ...pdf

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

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:

Jose Murry:

The book Applied Network Security Monitoring: Collection, Detection, and Analysis give you a sense of feeling enjoy for your spare time. You may use to make your capable much more increase. Book can to get your best friend when you getting strain or having big problem using your subject. If you can make reading a book Applied Network Security Monitoring: Collection, Detection, and Analysis to become your habit, you can get more advantages, like add your capable, increase your knowledge about a number of or all subjects. You may know everything if you like available and read a publication Applied Network Security

Monitoring: Collection, Detection, and Analysis. Kinds of book are a lot of. It means that, science publication or encyclopedia or some others. So , how do you think about this guide?

Richard Forbes:

This Applied Network Security Monitoring: Collection, Detection, and Analysis book is absolutely not ordinary book, you have after that it the world is in your hands. The benefit you receive by reading this book will be information inside this guide incredible fresh, you will get details which is getting deeper you actually read a lot of information you will get. That Applied Network Security Monitoring: Collection, Detection, and Analysis without we know teach the one who reading through it become critical in imagining and analyzing. Don't become worry Applied Network Security Monitoring: Collection, Detection, and Analysis can bring if you are and not make your bag space or bookshelves' grow to be full because you can have it in your lovely laptop even cell phone. This Applied Network Security Monitoring: Collection, Detection, and Analysis having great arrangement in word in addition to layout, so you will not truly feel uninterested in reading.

Brett Nash:

The book Applied Network Security Monitoring: Collection, Detection, and Analysis has a lot details on it. So when you check out this book you can get a lot of advantage. The book was written by the very famous author. The writer makes some research before write this book. This particular book very easy to read you may get the point easily after reading this article book.

Regina Dye:

As we know that book is very important thing to add our expertise for everything. By a publication we can know everything you want. A book is a set of written, printed, illustrated as well as blank sheet. Every year seemed to be exactly added. This book Applied Network Security Monitoring: Collection, Detection, and Analysis was filled in relation to science. Spend your time to add your knowledge about your research competence. Some people has several feel when they reading some sort of book. If you know how big advantage of a book, you can sense enjoy to read a reserve. In the modern era like today, many ways to get book that you just wanted.

Download and Read Online Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith #3D8RVHBG9LE

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

3D8RVHBG9LE: Applied Network Security Monitoring: Collection, Detection, and Analysis By Chris Sanders, Jason Smith