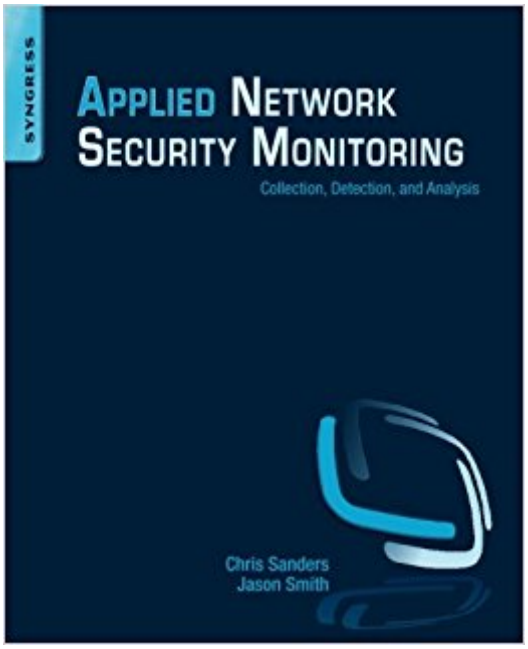
Applied Network Security Monitoring: Collection, Detection, And Analysis



Synopsis

Applied Network Security MonitoringÃ Â 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.Ã Â 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,Ã Â Applied Network Security MonitoringÃ Â 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 performingÃ Â 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.

Book Information

Paperback: 496 pages
Publisher: Syngress; 1 edition (December 19, 2013)
Language: English
ISBN-10: 0124172083
ISBN-13: 978-0124172081
Product Dimensions: 7.5 x 1.1 x 9.2 inches

Shipping Weight: 2.3 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 stars 33 customer reviews

Best Sellers Rank: #115,896 in Books (See Top 100 in Books) #83 inÃ Â Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs > Networks #145 inÃ Â Books > Computers & Technology > Networking & Cloud Computing > Network Security #202 inÃ Â Books > Textbooks > Computer Science > Networking

Customer Reviews

"... 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

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

Most enterprises split (as covered in the book) NSM into tiers up to three. This book will assist

anyone just getting in the field and help with foundational processes to unlock tier 2. Coverage of monitoring tools is spot on and does a decent job of proposing monitoring strategies. The book recommends good habits such as keeping an analyst journal and takes the perspective of an operator in the trenches.Would have liked to read about some novel approaches that leverage monitoring or, techniques to automate the most routine tasks but overall the book is an excellent desktop reference and guidance to NSM by analyst, for analyst.

book is brand new like the seller described it. no bends/dirts or nothing.

Disclaimers:IÃƒÂ¢Ã â ¬Ã â„¢m a long time NSM practitioner and I work with Smith & Bianco.Chris was gracious enough to provide me with a PDF copy of the book for review.- - - -Applied NSM is a powerhouse of practitioner knowledge. Divided into three primary sections (Collection, Detection, & Analysis) ANSM focuses on the key staples necessary for establishing a successful NSM program and how to get up and running.The book weighs in at an impressive 465 pages (including appendixes). However, depending on the readers familiarity with NSM and exposure to other related works on the subject, there could be some overlap.The areas I found most valuable that contributed new concepts to my ÃƒÂ¢Ã â ¬Ã Å“NSM library" included:Chapter 2ÃƒÂ¢Ã â ¬Ã â„¢s discussion on the Applied Collection FrameworkChapter 4ÃƒÂ¢Ã â ¬Ã â„¢s coverage of SiLK for analysis of flow dataChapter 6ÃƒÂ¢Ã â ¬Ã â„¢s coverage of LogStash and KibanaChapter 10ÃƒÂ¢Ã â ¬Ã â„¢s coverage on BroChapter 11ÃƒÂ¢Ã â ¬Ã â„¢s coverage on Anomaly based detection via SiLK toolsAppendix 3 makes for a handy desk side reference if you work with raw packet captures on a daily basis.For these sections alone, ANSM makes it well worth the purchase and addition to your collection. Speaking of which, all of the proceeds from this book go to several charities, and after having initially reviewed it for free, I still decided to purchase a copy on Kindle to have as a desk side reference and support such great causes.Great job guys!

Highly recommended! Applied NSM should be in every security professional’s bookshelf. Not only does it cover effective security monitoring methodologies and best practices, but walks you through from tool selection, installation, configuration, and maintenance.Overall, the book is very well written and carefully articulated; it almost leaves you without having to question or second guess the information provided. It just makes sense!

A must read for everyone working (or planning to work) to protect an operational network. Filled with

practical advice in building fundamental skills and solutions in environments with constrained budgets.

I purchased this book as part of a high level network monitoring project that I am working on within the Healthcare sector. This book was outstanding, if you want to learn about collection, detection and analysis of applied network security monitoring, this is the book for you. The content was outstanding, However I do have readers some advance warning. Please understand the basic dynamics of networking. This means please know the following Microsoft products, Cisco products etc. All the key important things a System Admin or Network Admin should already know. Please understand how to segment a network. Overall I found this book outstanding, I started reading the book when I received it. I am half way through the book, and thus far I like what I am reading. Great job.

I got this book a while ago and read first couple chapters and thought it was too easy, abstract and non-techinical. I assumed everything in this book is like that and boy, was I wrong. I actually read this book after I failed two incident response interviews and I realized that only if I had read this before I might have done better on the interviews. I'm not saying I could have got the job but I could have failed less miserably. Overall a really good book for people who have the basic networking knowledge, know some hex, binaries to do some packet analysis. If you are familiar with some packet capture tools or even NIDs that's an added advantage. If you are not familiar with computer networking then I would strongly suggest reading a networking book before you read this book, otherwise you will be lost.P.S. I really loved the chapter on Bro IDS.

Solid book for anyone who wants to build a network security program.

(Monographs in Oral Science, Vol. 21) Fetal Heart Monitoring Principles and Practices 4th Edition (Awhonn, Fetal Heart Monitoring) Fetal Heart Monitoring: Principles and Practices (AWHONN, Fetal Heart Monitoring) Monitoring Technologies in Acute Care Environments: A Comprehensive Guide to Patient Monitoring Technology Security Analysis: Sixth Edition, Foreword by Warren Buffett (Security Analysis Prior Editions) Access Control, Security, and Trust: A Logical Approach (Chapman & Hall/CRC Cryptography and Network Security Series) Handbook of Financial Cryptography and Security (Chapman & Hall/CRC Cryptography and Network Security Series) Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide CompTIA Security+ Guide to Network Security Fundamentals (with CertBlaster Printed Access Card) Security+ Guide to Network Security Fundamentals Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection (Wiley and SAS Business Series) Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security: Volume 28 NATO Science for Peace and Security Series - D: ... D: Information and Communication Security) Nuclear Safeguards, Security and Nonproliferation: Achieving Security with Technology and Policy (Butterworth-Heinemann Homeland Security) Security Camera For Home: Learn Everything About Wireless Security Camera System, Security Camera Installation and More Fundamentals Of Information Systems Security (Information Systems Security & Assurance) - Standalone book (Jones & Bartlett Learning Information Systems Security & Assurance)