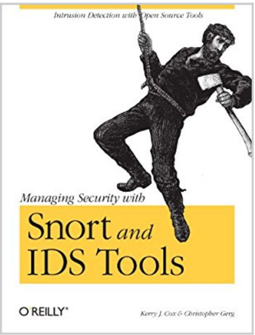
Intrusion Detection with Open Source Tools
Managing Security with
Snort and IDS Tools
O'REILLY
Kerry J. Cox & Christopher Gerg

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools

By Kerry J. Cox, Christopher Gerg

Download now

Read Online

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg

Intrusion detection is not for the faint at heart. But, if you are a network administrator chances are you're under increasing pressure to ensure that mission-critical systems are safe--in fact impenetrable--from malicious code, buffer overflows, stealth port scans, SMB probes, OS fingerprinting attempts, CGI attacks, and other network intruders.Designing a reliable way to detect intruders before they get in is a vital but daunting challenge. Because of this, a plethora of complex, sophisticated, and pricy software solutions are now available. In terms of raw power and features, SNORT, the most commonly used Open Source Intrusion Detection System, (IDS) has begun to eclipse many expensive proprietary IDSes. In terms of documentation or ease of use, however, SNORT can seem overwhelming. Which output plugin to use? How do you to email alerts to yourself? Most importantly, how do you sort through the immense amount of information Snort makes available to you?Many intrusion detection books are long on theory but short on specifics and practical examples. Not *Managing Security with Snort and IDS Tools*. This new book is a thorough, exceptionally practical guide to managing network security using Snort 2.1 (the latest release) and dozens of other high-quality open source other open source intrusion detection programs.*Managing Security with Snort and IDS Tools* covers reliable methods for detecting network intruders, from using simple packet sniffers to more sophisticated IDS (Intrusion Detection Systems) applications and the GUI interfaces for managing them. A comprehensive but concise guide for monitoring illegal entry attempts, this invaluable new book explains how to shut down and secure workstations, servers, firewalls, routers, sensors and other network devices.Step-by-step instructions are provided to quickly get up and running with Snort. Each chapter includes links for the programs discussed, and additional links at the end of the book give administrators access to numerous web sites for additional information and instructional material that will satisfy even the most serious security enthusiasts.*Managing Security with Snort and IDS Tools* maps out a proactive--and effective--approach to keeping your systems safe from attack.

Download Managing Security with Snort & IDS Tools: Intrusio ...pdf

Read Online Managing Security with Snort & IDS Tools: Intrus ...pdf

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools

By Kerry J. Cox, Christopher Gerg

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg

Intrusion detection is not for the faint at heart. But, if you are a network administrator chances are you're under increasing pressure to ensure that mission-critical systems are safe--in fact impenetrable--from malicious code, buffer overflows, stealth port scans, SMB probes, OS fingerprinting attempts, CGI attacks, and other network intruders.Designing a reliable way to detect intruders before they get in is a vital but daunting challenge. Because of this, a plethora of complex, sophisticated, and pricy software solutions are now available. In terms of raw power and features, SNORT, the most commonly used Open Source Intrusion Detection System, (IDS) has begun to eclipse many expensive proprietary IDSes. In terms of documentation or ease of use, however, SNORT can seem overwhelming. Which output plugin to use? How do you to email alerts to yourself? Most importantly, how do you sort through the immense amount of information Snort makes available to you?Many intrusion detection books are long on theory but short on specifics and practical examples. Not *Managing Security with Snort and IDS Tools*. This new book is a thorough, exceptionally practical guide to managing network security using Snort 2.1 (the latest release) and dozens of other high-quality open source other open source intrusion detection programs.*Managing Security with Snort and IDS Tools* covers reliable methods for detecting network intruders, from using simple packet sniffers to more sophisticated IDS (Intrusion Detection Systems) applications and the GUI interfaces for managing them. A comprehensive but concise guide for monitoring illegal entry attempts, this invaluable new book explains how to shut down and secure workstations, servers, firewalls, routers, sensors and other network devices.Step-by-step instructions are provided to quickly get up and running with Snort. Each chapter includes links for the programs discussed, and additional links at the end of the book give administrators access to numerous web sites for additional information and instructional material that will satisfy even the most serious security enthusiasts.*Managing Security with Snort and IDS Tools* maps out a proactive--and effective--approach to keeping your systems safe from attack.

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg Bibliography

- Rank: #395948 in eBooks
- Published on: 2004-08-02
- Released on: 2009-02-09
- Format: Kindle eBook

Download Managing Security with Snort & IDS Tools: Intrusio ...pdf

Read Online Managing Security with Snort & IDS Tools: Intrus ...pdf

Editorial Review

About the Author

Kerry Cox is a knowledgeable and enthusiastic chief administrator/network engineer at Bonneville International/KSL Radio and Television where he manages 40 Red Hat Linux servers, as well as Solaris and FreeBSD, performing installation, patching, hardening, and maintenance. He also handles all Cisco routers, switches, PIX and Checkpoint firewalls, CSS load balancers, IDS sensors and consoles. Kerry has implemented open source solution for monitoring networks, architectures, server processes, and bandwidth. Previously, he worked at network communications companies and ISPs and is the author of two books by Prima: the Linux Productivity Administrator's Guide and Red Hat Linux Administrator's Guide.

Christopher Gerg CISSP, CHSP is the Network Security Manager for Berbee Information Networks. His IT career started with phone technical support for Microsoft s launch of Windows 95 and his MCSE dates back to NT 3.51. He s worked as a system and network administrator and has traveled extensively installing WANs and infrastructure for a variety of clients. Five years ago things changed Christopher discovered open-source operating systems (FreeBSD, Debian, and Suse are his favorites) and he s spent three years as a penetration tester with Berbee and then transitioned from attack to defend for the last two years. Christopher is responsible for the network security of two Enterprise-class datacenters, the customers located in them, and the network infrastructure that connects it all (Multiple OC-48 SONET rings and multiple OC-3 s to the Internet). He uses Snort to watch it all.In his free time, Christopher raises rugged mountain alpacas in the wind-swept mountains of South-Central Wisconsin.

Users Review

From reader reviews:

Nancy Mitchell:

What do you concentrate on book? It is just for students since they're still students or the idea for all people in the world, the particular best subject for that? Only you can be answered for that concern above. Every person has diverse personality and hobby for every single other. Don't to be pressured someone or something that they don't need do that. You must know how great as well as important the book Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools. All type of book could you see on many options. You can look for the internet solutions or other social media.

Michele Anderson:

People live in this new time of lifestyle always aim to and must have the extra time or they will get large amount of stress from both day to day life and work. So , once we ask do people have extra time, we will say absolutely without a doubt. People is human not a robot. Then we question again, what kind of activity are there when the spare time coming to an individual of course your answer will probably unlimited right. Then do you try this one, reading textbooks. It can be your alternative with spending your spare time, often the book you have read is Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools.

Ernest Bryan:

Are you kind of stressful person, only have 10 or perhaps 15 minute in your morning to upgrading your mind talent or thinking skill possibly analytical thinking? Then you are receiving problem with the book than can satisfy your limited time to read it because this time you only find book that need more time to be study. Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools can be your answer since it can be read by anyone who have those short time problems.

Bess Cook:

Don't be worry should you be afraid that this book can filled the space in your house, you will get it in e-book approach, more simple and reachable. This Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools can give you a lot of buddies because by you checking out this one book you have point that they don't and make a person more like an interesting person. This particular book can be one of one step for you to get success. This guide offer you information that maybe your friend doesn't learn, by knowing more than other make you to be great persons. So , why hesitate? Let us have Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools.

Download and Read Online Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg #1CBMXSFPTLO

Read Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg for online ebook

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg 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 Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg books to read online.

Online Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg ebook PDF download

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg Doc

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg Mobipocket

Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools By Kerry J. Cox, Christopher Gerg EPub