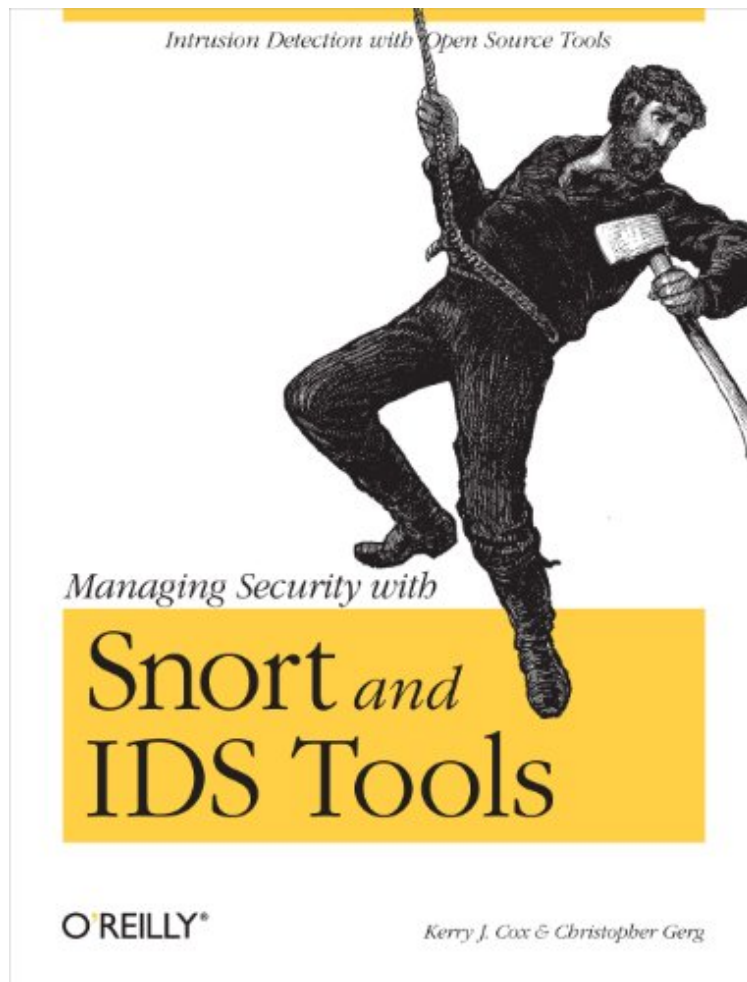


Managing Security with Snort IDS Tools: Intrusion Detection with Open Source Tools

Von Kerry J. Cox, Christopher Gerg
DOC | *audiobook | ebooks | Download PDF | ePub



DOWNLOAD



READ ONLINE

Produktinformation -Verkaufsrang: #710069 in eBooksVerffentlicht am: 2004-08-02Erscheinungsdatum:
2009-02-09File Name: B0043EWW0Q | File size: 23.Mb

Von Kerry J. Cox, Christopher Gerg : Managing Security with Snort IDS Tools: Intrusion Detection with Open Source Tools before purchasing it in order to gage whether or not it would be worth my time, and all praised Managing Security with Snort IDS Tools: Intrusion Detection with Open Source Tools:

KundenrezensionenHilfreichste Kundenrezensionen1 von 2 Kunden fanden die folgende Rezension hilfreich. Gutes Buuch, aber teilweise zuviel KonfigurationsdateienVon Sebastian BickelNach dem Buch kennt man sicherlich alles im Zusammenhang mit Snort. Allerdings hte ich mir gwnscht, dass der Author weniger Konfigurationsdateien abdruckt und mehr noch auf verschiedene Implementierungsstrategien eingeht.

Kurzbeschreibung 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.

Kurzbeschreibung 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.