OSSEC Host-Based Intrusion Detection Guide

Andrew Hay, Daniel Cid, Rory Bray

OSSEC Host-Based Intrusion Detection Guide

Andrew Hay, Daniel Cid, Rory Bray

OSSEC Host-Based Intrusion Detection Guide Andrew Hay, Daniel Cid, Rory Bray

This book is the definitive guide on the OSSEC Host-based Intrusion Detection system and frankly, to really use OSSEC you are going to need a definitive guide. Documentation has been available since the start of the OSSEC project but, due to time constraints, no formal book has been created to outline the various features and functions of the OSSEC product. This has left very important and powerful features of the product undocumented...until now! The book you are holding will show you how to install and configure OSSEC on the operating system of your choice and provide detailed examples to help prevent and mitigate attacks on your systems. -- Stephen Northcutt OSSEC determines if a host has been compromised in this manner by taking the equivalent of a picture of the host machine in its original, unaltered state. This "picture" captures the most relevant information about that machine's configuration. OSSEC saves this "picture" and then constantly compares it to the current state of that machine to identify anything that may have changed from the original configuration. Now, many of these changes are necessary, harmless, and authorized, such as a system administrator installing a new software upgrade, patch, or application. But, then there are the not-so-harmless changes, like the installation of a rootkit, trojan horse, or virus. Differentiating between the harmless and the not-so-harmless changes determines whether the system administrator or security professional is managing a secure, efficient network or a compromised network which might be funneling credit card numbers out to phishing gangs or storing massive amounts of pornography creating significant liability for that organization. Separating the wheat from the chaff is by no means an easy task. Hence the need for this book. The book is co-authored by Daniel Cid, who is the founder and lead developer of the freely available OSSEC host-based IDS. As such, readers can be certain they are reading the most accurate, timely, and insightful information on OSSEC.

All disc-based content for this title is now available on the Web.

* **Nominee for Best Book Bejtlich read in 2008!**
* http://taosecurity.blogspot.com/2008/12/best-book-bejtlich-read-in-2008.html

• Get Started with OSSEC
Get an overview of the features of OSSEC including commonly used terminology, pre-install preparation, and deployment considerations.
• Follow Steb-by-Step Installation Instructions
Walk through the installation process for the "local”, “agent”, and "server" install types on some of the most popular operating systems available.
• Master Configuration
Learn the basic configuration options for your install type and learn how to monitor log files, receive remote messages, configure email notification, and configure alert levels.
• Work With Rules
Extract key information from logs using decoders and how you can leverage rules to alert you of strange occurrences on your network.
• Understand System Integrity Check and Rootkit Detection

Monitor binary executable files, system configuration files, and the Microsoft Windows registry.
• Configure Active Response
Configure the active response actions you want and bind the actions to specific rules and sequence of events.
• Use the OSSEC Web User Interface
Install, configure, and use the community-developed, open source web interface available for OSSEC.
• Play in the OSSEC VMware Environment Sandbox
• Dig Deep into Data Log Mining
Take the “high art” of log analysis to the next level by breaking the dependence on the lists of strings or patterns to look for in the logs.

Download and Read Free Online OSSEC Host-Based Intrusion Detection Guide Andrew Hay, Daniel Cid, Rory Bray

---

From reader reviews:

Lenore Ryan:

Why don't make it to be your habit? Right now, try to prepare your time to do the important work, like looking for your favorite publication and reading a reserve. Beside you can solve your short lived problem; you can add your knowledge by the publication entitled OSSEC Host-Based Intrusion Detection Guide. Try to make the book OSSEC Host-Based Intrusion Detection Guide as your buddy. It means that it can to become your friend when you experience alone and beside that of course make you smarter than in the past. Yeah, it is very fortuned for yourself. The book makes you much more confidence because you can know every little thing by the book. So , let me make new experience and also knowledge with this book.

Blake Nixon:

Book is to be different for each grade. Book for children until adult are different content. To be sure that book is very important normally. The book OSSEC Host-Based Intrusion Detection Guide ended up being making you to know about other understanding and of course you can take more information. It is quite advantages for you. The e-book OSSEC Host-Based Intrusion Detection Guide is not only giving you far more new information but also to become your friend when you experience bored. You can spend your own personal spend time to read your publication. Try to make relationship with the book OSSEC Host-Based Intrusion Detection Guide. You never truly feel lose out for everything in the event you read some books.

Mary Norman:

You are able to spend your free time to see this book this publication. This OSSEC Host-Based Intrusion Detection Guide is simple to create you can read it in the park your car, in the beach, train and soon. If you did not have much space to bring often the printed book, you can buy the e-book. It is make you much easier to read it. You can save the book in your smart phone. So there are a lot of benefits that you will get when one buys this book.

Brianna Bell:

Beside that OSSEC Host-Based Intrusion Detection Guide in your phone, it can give you a way to get closer to the new knowledge or facts. The information and the knowledge you might got here is fresh in the oven so don't end up being worry if you feel like an outdated people live in narrow commune. It is good thing to have OSSEC Host-Based Intrusion Detection Guide because this book offers to you personally readable information. Do you oftentimes have book but you would not get what it's interesting features of. Oh come on, that will not happen if you have this in the hand. The Enjoyable option here cannot be questionable, similar to treasuring beautiful island. Techniques you still want to miss this? Find this book and read it from at this point!

Read OSSEC Host-Based Intrusion Detection Guide by Andrew Hay, Daniel Cid, Rory Bray for online ebook

OSSEC Host-Based Intrusion Detection Guide by Andrew Hay, Daniel Cid, Rory Bray 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 OSSEC Host-Based Intrusion Detection Guide by Andrew Hay, Daniel Cid, Rory Bray books to read online.

Online OSSEC Host-Based Intrusion Detection Guide by Andrew Hay, Daniel Cid, Rory Bray ebook PDF download

OSSEC Host-Based Intrusion Detection Guide by Andrew Hay, Daniel Cid, Rory Bray Doc

OSSEC Host-Based Intrusion Detection Guide by Andrew Hay, Daniel Cid, Rory Bray Mobipocket

OSSEC Host-Based Intrusion Detection Guide by Andrew Hay, Daniel Cid, Rory Bray EPub