OSSEC Host-Based Intrusion Detection Guide

Andrew Hay

OSSEC Host-Based Intrusion Detection Guide

Andrew Hay

OSSEC Host-Based Intrusion Detection Guide Andrew Hay

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

---

From reader reviews:

Michael Brown:

As people who live in the particular modest era should be upgrade about what going on or information even knowledge to make these people keep up with the era that is always change and advance. Some of you maybe may update themselves by looking at books. It is a good choice for you personally but the problems coming to an individual is you don't know what type you should start with. This OSSEC Host-Based Intrusion Detection Guide is our recommendation to cause you to keep up with the world. Why, because book serves what you want and want in this era.

Robert Hicks:

Hey guys, do you would like to finds a new book to see? May be the book with the concept OSSEC Host-Based Intrusion Detection Guide suitable to you? Often the book was written by famous writer in this era. Typically the book untitled OSSEC Host-Based Intrusion Detection Guideis the one of several books in which everyone read now. This kind of book was inspired a lot of people in the world. When you read this reserve you will enter the new age that you ever know ahead of. The author explained their plan in the simple way, therefore all of people can easily to know the core of this publication. This book will give you a lot of information about this world now. To help you to see the represented of the world with this book.

Ann Conley:

That e-book can make you to feel relax. This specific book OSSEC Host-Based Intrusion Detection Guide was multi-colored and of course has pictures on there. As we know that book OSSEC Host-Based Intrusion Detection Guide has many kinds or category. Start from kids until young adults. For example Naruto or Investigation company Conan you can read and believe that you are the character on there. So , not at all of book tend to be make you bored, any it offers up you feel happy, fun and loosen up. Try to choose the best book in your case and try to like reading in which.

Frances Pierce:

Reading a book make you to get more knowledge from that. You can take knowledge and information originating from a book. Book is composed or printed or outlined from each source that will filled update of news. On this modern era like today, many ways to get information are available for you actually. From media social like newspaper, magazines, science book, encyclopedia, reference book, book and comic. You can add your knowledge by that book. Are you ready to spend your spare time to spread out your book? Or just in search of the OSSEC Host-Based Intrusion Detection Guide when you needed it?

Read OSSEC Host-Based Intrusion Detection Guide by Andrew Hay for online ebook

OSSEC Host-Based Intrusion Detection Guide by Andrew Hay 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 books to read online.

Online OSSEC Host-Based Intrusion Detection Guide by Andrew Hay ebook PDF download

OSSEC Host-Based Intrusion Detection Guide by Andrew Hay Doc

OSSEC Host-Based Intrusion Detection Guide by Andrew Hay Mobipocket

OSSEC Host-Based Intrusion Detection Guide by Andrew Hay EPub