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:

Serina Horne:

Information is provisions for anyone to get better life, information these days can get by anyone in everywhere. The information can be a expertise or any news even an issue. What people must be consider while those information which is inside the former life are hard to be find than now is taking seriously which one is appropriate to believe or which one the actual resource are convinced. If you get the unstable resource then you have it as your main information we will see huge disadvantage for you. All of those possibilities will not happen with you if you take OSSEC Host-Based Intrusion Detection Guide as your daily resource information.

Amy Dixon:

Reading a publication tends to be new life style on this era globalization. With reading you can get a lot of information which will give you benefit in your life. With book everyone in this world can share their idea. Guides can also inspire a lot of people. A lot of author can inspire their very own reader with their story or maybe their experience. Not only the story that share in the books. But also they write about the ability about something that you need illustration. How to get the good score toefl, or how to teach your children, there are many kinds of book that exist now. The authors nowadays always try to improve their talent in writing, they also doing some study before they write with their book. One of them is this OSSEC Host-Based Intrusion Detection Guide.

Tammy Jones:

Are you kind of hectic person, only have 10 or perhaps 15 minute in your day time to upgrading your mind skill or thinking skill perhaps analytical thinking? Then you are experiencing problem with the book than can satisfy your short period of time to read it because pretty much everything time you only find e-book that need more time to be examine. OSSEC Host-Based Intrusion Detection Guide can be your answer mainly because it can be read by you who have those short time problems.

Pearl Minjares:

This OSSEC Host-Based Intrusion Detection Guide is completely new way for you who has interest to look for some information as it relief your hunger info. Getting deeper you upon it getting knowledge more you know or else you who still having tiny amount of digest in reading this OSSEC Host-Based Intrusion Detection Guide can be the light food for you because the information inside that book is easy to get by means of anyone. These books develop itself in the form which can be reachable by anyone, sure I mean in the e-book application form. People who think that in reserve form make them feel sleepy even dizzy this e-book is the answer. So there is not any in reading a e-book especially this one. You can find actually looking for. It should be here for an individual. So , don't miss this! Just read this e-book variety for your better life in addition to knowledge.

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