Google Drive

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:

Elisabeth Martinez:

Hey guys, do you wants to finds a new book you just read? May be the book with the subject OSSEC Host-Based Intrusion Detection Guide suitable to you? Often the book was written by well known writer in this era. Typically the book untitled OSSEC Host-Based Intrusion Detection Guideis the main of several books that everyone read now. This specific book was inspired many men and women in the world. When you read this publication you will enter the new dimensions that you ever know previous to. The author explained their strategy in the simple way, therefore all of people can easily to understand the core of this book. This book will give you a lots of information about this world now. In order to see the represented of the world with this book.

Edward Stevenson:

Do you one of the book lovers? If yes, do you ever feeling doubt if you are in the book store? Try to pick one book that you just dont know the inside because don't judge book by its include may doesn't work the following is difficult job because you are scared that the inside maybe not since fantastic as in the outside appearance likes. Maybe you answer may be OSSEC Host-Based Intrusion Detection Guide why because the great cover that make you consider with regards to the content will not disappoint anyone. The inside or content will be fantastic as the outside as well as cover. Your reading sixth sense will directly make suggestions to pick up this book.

Brooks Davis:

Beside that OSSEC Host-Based Intrusion Detection Guide in your phone, it could give you a way to get closer to the new knowledge or data. The information and the knowledge you can got here is fresh through the oven so don't possibly be worry if you feel like an previous people live in narrow small town. It is good thing to have OSSEC Host-Based Intrusion Detection Guide because this book offers to you readable information. Do you sometimes 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 your hand. The Enjoyable agreement here cannot be questionable, including treasuring beautiful island. Techniques you still want to miss it? Find this book and also read it from today!

Mary Linkous:

This OSSEC Host-Based Intrusion Detection Guide is completely new way for you who has intense curiosity to look for some information mainly because it relief your hunger of knowledge. Getting deeper you on it getting knowledge more you know or else you who still having little bit of digest in reading this OSSEC Host-Based Intrusion Detection Guide can be the light food to suit your needs because the information inside this book is easy to get by simply anyone. These books produce itself in the form that is reachable by anyone, that's why I mean in the e-book contact form. People who think that in e-book form make them feel sleepy even dizzy this e-book is the answer. So there isn't any in reading a reserve especially this one. You can find actually looking for. It should be here for you. So , don't miss the item! Just read this e-book variety for your better life and also knowledge.

Download and Read Online OSSEC Host-Based Intrusion Detection Guide Andrew Hay #4ORUWH0GEQB

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