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:

Betty Lavery:

What do you with regards to book? It is not important along? Or just adding material if you want something to explain what you problem? How about your spare time? Or are you busy man? If you don't have spare time to complete others business, it is gives you the sense of being bored faster. And you have time? What did you do? Every person has many questions above. They need to answer that question because just their can do that. It said that about publication. Book is familiar in each person. Yes, it is proper. Because start from on kindergarten until university need this specific OSSEC Host-Based Intrusion Detection Guide to read.

Oliver Watts:

Nowadays reading books become more than want or need but also get a life style. This reading practice give you lot of advantages. The huge benefits you got of course the knowledge even the information inside the book in which improve your knowledge and information. The knowledge you get based on what kind of guide you read, if you want attract knowledge just go with schooling books but if you want really feel happy read one using theme for entertaining such as comic or novel. The OSSEC Host-Based Intrusion Detection Guide is kind of e-book which is giving the reader unpredictable experience.

Delores Keener:

Reading can called head hangout, why? Because if you find yourself reading a book especially book entitled OSSEC Host-Based Intrusion Detection Guide your brain will drift away trough every dimension, wandering in each and every aspect that maybe not known for but surely will become your mind friends. Imaging every word written in a guide then become one application form conclusion and explanation this maybe you never get prior to. The OSSEC Host-Based Intrusion Detection Guide giving you a different experience more than blown away the mind but also giving you useful info for your better life with this era. So now let us demonstrate the relaxing pattern this is your body and mind will be pleased when you are finished reading through it, like winning a game. Do you want to try this extraordinary investing spare time activity?

Wiley Wagner:

A lot of reserve has printed but it is unique. You can get it by world wide web on social media. You can choose the best book for you, science, comedian, novel, or whatever by means of searching from it. It is known as of book OSSEC Host-Based Intrusion Detection Guide. You can add your knowledge by it. Without departing the printed book, it can add your knowledge and make you happier to read. It is most important that, you must aware about e-book. It can bring you from one spot to other place.

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

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

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