Google Drive



Instant OSSEC Host-based Intrusion Detection System

Brad Lhotsky

Download now

Click here if your download doesn"t start automatically

Instant OSSEC Host-based Intrusion Detection System

Brad Lhotsky

Instant OSSEC Host-based Intrusion Detection System Brad Lhotsky

A hands-on guide exploring OSSEC HIDS for operational and security awareness

Overview

- Learn something new in an Instant! A short, fast, focused guide delivering immediate results
- Install, configure, and customize an OSSEC-HIDS for your environment
- Manage your OSSEC-HIDS robust and comprehensive security checks
- Write your own rules and decoders to enhance alert accuracy and expand operational and security intelligence

In Detail

Security software is often expensive, restricting, burdensome, and noisy. OSSEC-HIDS was designed to avoid getting in your way and to allow you to take control of and extract real value from industry security requirements. OSSEC-HIDS is a comprehensive, robust solution to many common security problems faced in organizations of all sizes.

"Instant OSSEC-HIDS" is a practical guide to take you from beginner to power user through recipes designed based on real- world experiences. Recipes are designed to provide instant impact while containing enough detail to allow the reader to further explore the possibilities. Using real world examples, this book will take you from installing a simple, local OSSEC-HIDS service to commanding a network of servers running OSSEC-HIDS with customized checks, alerts, and automatic responses.

You will learn how to maximise the accuracy, effectiveness, and performance of OSSEC-HIDS' analyser, file integrity monitor, and malware detection module. You will flip the table on security software and put OSSEC-HIDS to work validating its own alerts before escalating them. You will also learn how to write your own rules, decoders, and active responses. You will rest easy knowing your servers can protect themselves from most attacks while being intelligent enough to notify you when they need help!

You will learn how to use OSSEC-HIDS to save time, meet security requirements, provide insight into your network, and protect your assets.

What you will learn from this book

- Installing OSSEC-HIDS in local, server, and agent mode
- Customizing alerting to increase the signal to noise ratio
- Writing your own rules to extend, enhance, and tailor alerts to your environment
- Writing your own decoders to add context to alerts and active responses
- Learning tips for managing large OSSEC-HIDS installs
- Monitoring command output for security and operational awareness
- Auditing systems for compromise with a sensitivity to performance of those systems
- Configuring Active Response to protect servers from SSH brute force attacks

Approach

Filled with practical, step-by-step instructions and clear explanations for the most important and useful tasks. A fast-paced, practical guide to OSSEC-HIDS that will help you solve host-based security problems.

Who this book is written for

This book is great for anyone concerned about the security of their servers-whether you are a system administrator, programmer, or security analyst, this book will provide you with tips to better utilize OSSEC-HIDS. Whether you're new to OSSEC-HIDS or a seasoned veteran, you'll find something in this book you can apply today!

This book assumes some knowledge of basic security concepts and rudimentary scripting experience.

Download Instant OSSEC Host-based Intrusion Detection Syste ...pdf

Read Online Instant OSSEC Host-based Intrusion Detection Sys ...pdf

Download and Read Free Online Instant OSSEC Host-based Intrusion Detection System Brad Lhotsky

---

From reader reviews:

Ian Ashlock:

The book Instant OSSEC Host-based Intrusion Detection System give you a sense of feeling enjoy for your spare time. You need to use to make your capable much more increase. Book can to be your best friend when you getting tension or having big problem with the subject. If you can make reading a book Instant OSSEC Host-based Intrusion Detection System being your habit, you can get far more advantages, like add your personal capable, increase your knowledge about a number of or all subjects. You could know everything if you like available and read a e-book Instant OSSEC Host-based Intrusion Detection System. Kinds of book are a lot of. It means that, science e-book or encyclopedia or others. So , how do you think about this e-book?

Ramon Hudson:

The reserve with title Instant OSSEC Host-based Intrusion Detection System has a lot of information that you can understand it. You can get a lot of benefit after read this book. That book exist new knowledge the information that exist in this guide represented the condition of the world today. That is important to yo7u to find out how the improvement of the world. This specific book will bring you throughout new era of the the positive effect. You can read the e-book on your own smart phone, so you can read that anywhere you want.

Larry Chaffin:

Do you one of the book lovers? If yes, do you ever feeling doubt when you are in the book store? Aim to pick one book that you find out the inside because don't assess book by its protect may doesn't work the following is difficult job because you are scared that the inside maybe not while fantastic as in the outside search likes. Maybe you answer might be Instant OSSEC Host-based Intrusion Detection System why because the fantastic cover that make you consider regarding the content will not disappoint anyone. The inside or content is actually fantastic as the outside or even cover. Your reading sixth sense will directly make suggestions to pick up this book.

Awilda Kell:

Are you kind of stressful person, only have 10 as well as 15 minute in your moment to upgrading your mind talent or thinking skill possibly analytical thinking? Then you are experiencing problem with the book when compared with can satisfy your short space of time to read it because all this time you only find e-book that need more time to be go through. Instant OSSEC Host-based Intrusion Detection System can be your answer mainly because it can be read by a person who have those short spare time problems.

Download and Read Online Instant OSSEC Host-based Intrusion Detection System Brad Lhotsky #69XI4UR8KMZ

Read Instant OSSEC Host-based Intrusion Detection System by Brad Lhotsky for online ebook

Instant OSSEC Host-based Intrusion Detection System by Brad Lhotsky 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 Instant OSSEC Host-based Intrusion Detection System by Brad Lhotsky books to read online.

Online Instant OSSEC Host-based Intrusion Detection System by Brad Lhotsky ebook PDF download

Instant OSSEC Host-based Intrusion Detection System by Brad Lhotsky Doc

Instant OSSEC Host-based Intrusion Detection System by Brad Lhotsky Mobipocket

Instant OSSEC Host-based Intrusion Detection System by Brad Lhotsky EPub