Instant OSSEC Host-based Intrusion Detection System

Brad Lhotsky

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

---

From reader reviews:

Matthew Lyons:

Why don't make it to be your habit? Right now, try to prepare your time to do the important action, like looking for your favorite book and reading a guide. Beside you can solve your short lived problem; you can add your knowledge by the publication entitled Instant OSSEC Host-based Intrusion Detection System. Try to face the book Instant OSSEC Host-based Intrusion Detection System as your friend. It means that it can to be your friend when you truly feel alone and beside that of course make you smarter than in the past. Yeah, it is very fortuned for you personally. The book makes you a lot more confidence because you can know almost everything by the book. So , let us make new experience as well as knowledge with this book.

Angelita Estes:

Book is to be different for every grade. Book for children right up until adult are different content. As we know that book is very important usually. The book Instant OSSEC Host-based Intrusion Detection System has been making you to know about other information and of course you can take more information. It doesn't matter what advantages for you. The reserve Instant OSSEC Host-based Intrusion Detection System is not only giving you considerably more new information but also to become your friend when you experience bored. You can spend your own personal spend time to read your e-book. Try to make relationship using the book Instant OSSEC Host-based Intrusion Detection System. You never sense lose out for everything if you read some books.

Dennis Johnson:

Playing with family in the park, coming to see the sea world or hanging out with close friends is thing that usually you could have done when you have spare time, in that case why you don't try issue that really opposite from that. A single activity that make you not experiencing tired but still relaxing, trilling like on roller coaster you already been ride on and with addition details. Even you love Instant OSSEC Host-based Intrusion Detection System, it is possible to enjoy both. It is very good combination right, you still want to miss it? What kind of hang type is it? Oh come on its mind hangout people. What? Still don't obtain it, oh come on its identified as reading friends.

Claudette Everett:

Do you one of the book lovers? If yes, do you ever feeling doubt if you are in the book store? Try and pick one book that you never know the inside because don't judge book by its deal with may doesn't work here is difficult job because you are afraid that the inside maybe not because fantastic as in the outside look likes. Maybe you answer might be Instant OSSEC Host-based Intrusion Detection System why because the excellent cover that make you consider with regards to the content will not disappoint anyone. The inside or content is usually fantastic as the outside or cover. Your reading 6th sense will directly direct you to pick up this book.

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