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:

Steven Maravilla:

Nowadays reading books are more than want or need but also turn into a life style. This reading habit give you lot of advantages. The huge benefits you got of course the knowledge the rest of the information inside the book that improve your knowledge and information. The info you get based on what kind of guide you read, if you want drive more knowledge just go with education and learning books but if you want sense happy read one together with theme for entertaining such as comic or novel. The actual Instant OSSEC Host-based Intrusion Detection System is kind of book which is giving the reader unpredictable experience.

Susan Burroughs:

Reading a book can be one of a lot of action that everyone in the world adores. Do you like reading book therefore. There are a lot of reasons why people enjoyed. First reading a guide will give you a lot of new data. When you read a reserve you will get new information simply because book is one of a number of ways to share the information or perhaps their idea. Second, looking at a book will make anyone more imaginative. When you reading a book especially fictional book the author will bring one to imagine the story how the characters do it anything. Third, you can share your knowledge to others. When you read this Instant OSSEC Host-based Intrusion Detection System, it is possible to tells your family, friends and soon about yours publication. Your knowledge can inspire the mediocre, make them reading a reserve.

Ernest Nunez:

Do you really one of the book lovers? If yes, do you ever feeling doubt while you are in the book store? Try to pick one book that you find out the inside because don't assess book by its deal with may doesn't work at this point is difficult job because you are afraid that the inside maybe not since fantastic as in the outside appear likes. Maybe you answer might be Instant OSSEC Host-based Intrusion Detection System why because the great cover that make you consider regarding the content will not disappoint an individual. The inside or content will be fantastic as the outside or cover. Your reading sixth sense will directly show you to pick up this book.

Karin Decker:

Are you kind of busy person, only have 10 or 15 minute in your day to upgrading your mind proficiency or thinking skill possibly analytical thinking? Then you have problem with the book as compared to can satisfy your limited time to read it because all this time you only find book that need more time to be read. Instant OSSEC Host-based Intrusion Detection System can be your answer as it can be read by an individual who have those short extra time problems.

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