Instant OSSEC Host-based Intrusion Detection System

By Brad Lhotsky

Download now

Read Online

Instant OSSEC Host-based Intrusion Detection System By 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

Instant OSSEC Host-based Intrusion Detection System

By Brad Lhotsky

Instant OSSEC Host-based Intrusion Detection System By 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.

Instant OSSEC Host-based Intrusion Detection System By Brad Lhotsky Bibliography

- Sales Rank: #1493750 in Books
- Published on: 2013-07-26
- Released on: 2013-07-26
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .14" w x 7.50" l, .27 pounds
- Binding: Paperback
- 62 pages

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 By Brad Lhotsky

---

Editorial Review

About the Author

Brad Lhotsky

Brad Lhotsky started working with UNIX systems professionally in 1998 as a system administrator, database administrator, network engineer, programmer, and security administrator. He has been an active member of the OSSEC-HIDS community since 2004. He also currently administers one of the largest OSSEC-HIDS deployments in the world!

Users Review

From reader reviews:

Frank Hegarty:

Here thing why this specific Instant OSSEC Host-based Intrusion Detection System are different and reputable to be yours. First of all examining a book is good however it depends in the content of the usb ports which is the content is as scrumptious as food or not. Instant OSSEC Host-based Intrusion Detection System giving you information deeper as different ways, you can find any e-book out there but there is no reserve that similar with Instant OSSEC Host-based Intrusion Detection System. It gives you thrill studying journey, its open up your own personal eyes about the thing in which happened in the world which is perhaps can be happened around you. It is easy to bring everywhere like in park, café, or even in your way home by train. In case you are having difficulties in bringing the imprinted book maybe the form of Instant OSSEC Host-based Intrusion Detection System in e-book can be your substitute.

Angel Sherrill:

This book untitled Instant OSSEC Host-based Intrusion Detection System to be one of several books that best seller in this year, that is because when you read this book you can get a lot of benefit on it. You will easily to buy this specific book in the book retailer or you can order it by using online. The publisher on this book sells the e-book too. It makes you quickly to read this book, since you can read this book in your Mobile phone. So there is no reason for you to past this publication from your list.

Walter Reeves:

A lot of people always spent their particular free time to vacation or go to the outside with them family members or their friend. Do you realize? Many a lot of people spent they will free time just watching TV, or perhaps playing video games all day long. If you need to try to find a new activity honestly, that is look different you can read any book. It is really fun to suit your needs. If you enjoy the book that you just read you can spent all day every day to reading a e-book. The book Instant OSSEC Host-based Intrusion Detection System it doesn't matter what good to read. There are a lot of individuals who recommended this

book. These were enjoying reading this book. If you did not have enough space to create this book you can buy often the e-book. You can m0ore very easily to read this book from your smart phone. The price is not to cover but this book possesses high quality.

Terrie Anderson:

As a scholar exactly feel bored to help reading. If their teacher requested them to go to the library or even make summary for some book, they are complained. Just minor students that has reading's heart and soul or real their interest. They just do what the educator want, like asked to go to the library. They go to right now there but nothing reading critically. Any students feel that looking at is not important, boring as well as can't see colorful photographs on there. Yeah, it is to become complicated. Book is very important in your case. As we know that on this era, many ways to get whatever we wish. Likewise word says, many ways to reach Chinese's country. Therefore , this Instant OSSEC Host-based Intrusion Detection System can make you really feel more interested to read.

Download and Read Online Instant OSSEC Host-based Intrusion Detection System By Brad Lhotsky #IY95OZULJWF

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

IY95OZULJWF: Instant OSSEC Host-based Intrusion Detection System By Brad Lhotsky