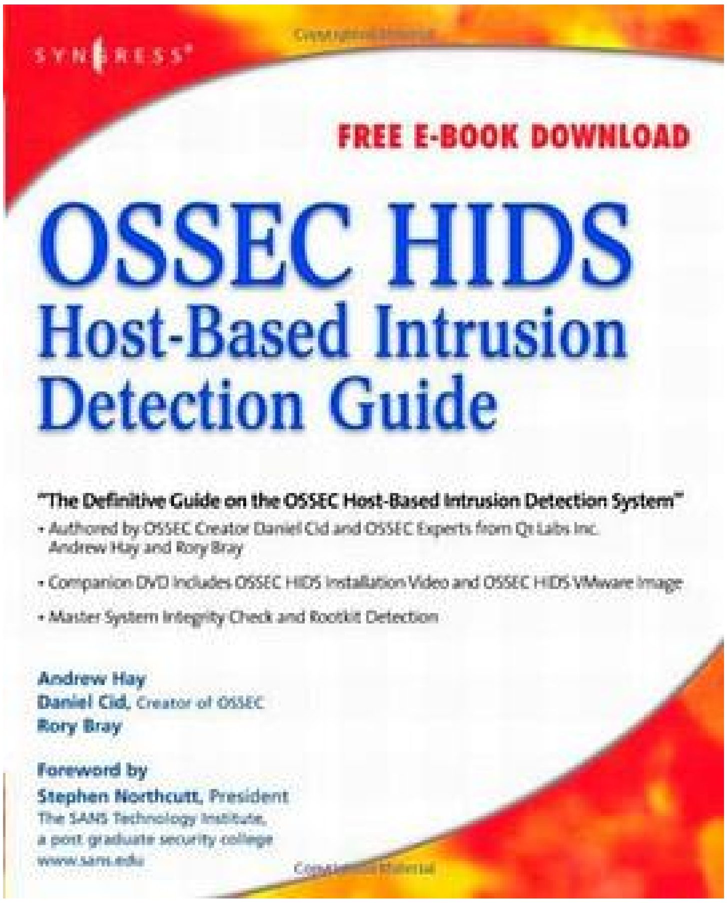
OSSEC Host-Based Intrusion Detection Guide



OSSEC Host-Based Intrusion Detection Guide_下载链接1_

著者:Andrew Hay

出版者:Syngress

出版时间:2008-3-17

装帧:Paperback

isbn:9781597492409

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.

* 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

Use the OSSEC HIDS VMware Guest image on the companion DVD to implement what you have learned in a sandbox-style environment.

. 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.

作者介绍:

目录:

OSSEC Host-Based Intrusion Detection Guide_下载链接1_

标签

网络安全

日志分析

入侵检测

评论

内容不是很新,很好的指导书.

OSSEC Host-Based Intrusion Detection Guide_下载链接1_

书评

OSSEC Host-Based Intrusion Detection Guide_下载链接1_