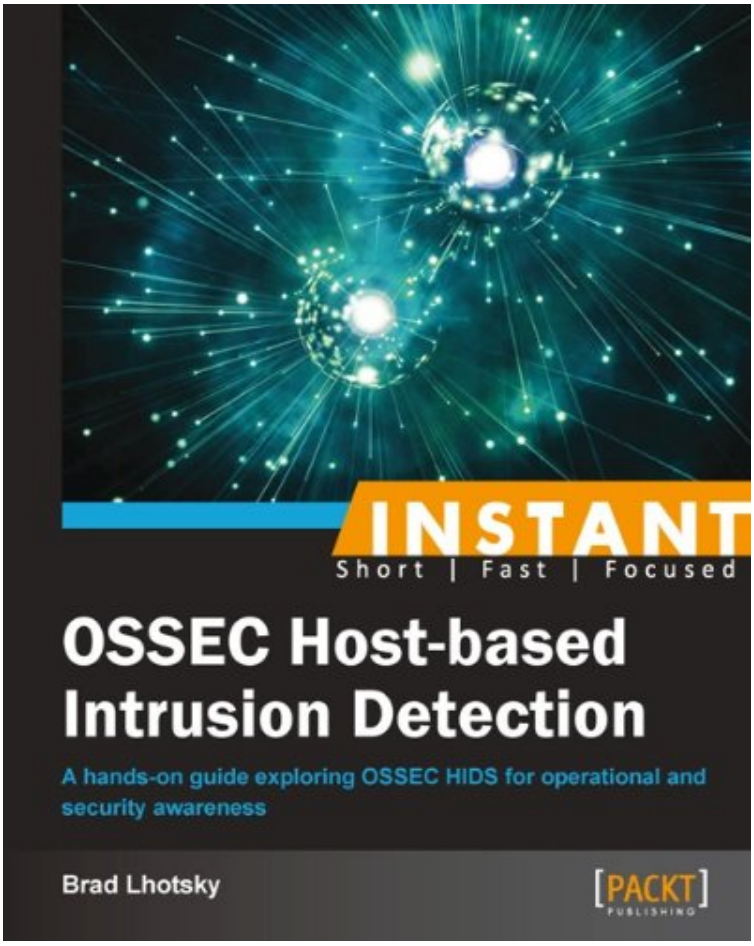
Instant OSSEC Host-based Intrusion Detection

Von Brad Lhotsky
**Download PDF | ePub | DOC | audiobook | ebooks*



Produktinformation -Verkaufsrang: #401518 in eBooksVerffentlicht am: 2013-08-22Erscheinungsdatum: 2013-08-22File Name: B00E7NC9K0 | File size: 53.Mb

Von Brad Lhotsky : Instant OSSEC Host-based Intrusion Detection before purchasing it in order to gage whether or not it would be worth my time, and all praised Instant OSSEC Host-based Intrusion Detection:

KundenrezensionenHilfreichste Kundenrezensionen0 von 0 Kunden fanden die folgende Rezension hilfreich. A very helpful quickstart guide and beyondVon Thomas WidhalmFirst of all I want to say that I'm thankful for the opportunity to review a free copy of this book. I will try to not get biased towards this book by this circumstance.OSSEC HIDS is a host based intrusion detection system with 2 main differences to similar systems. OSSEC has a simple method of responding to detected intrusions (blocking offending hosts via local firewall or route configuration) and is a simple intrusion prevention system as well. Furthermore OSSEC uses a client-server model which does not only provide easy centralised configuration management but enables ossec to block offending hosts on all clients even when only one of them detects the intrusion attempt. While it is clearly a Linux / Unix tool, OSSECs client can run on Microsoft Windows hosts, too.Like any IDS/IPS system OSSEC is no easily set up fire-and-forget solution but a complex system which needs know-how to implement and run it. A book of this size can not be a full

manual but it is a very good quickstart guide. OSSEC has to be installed and configured before you can dive into creating your own decoders (how to get information out of your logfiles), rules (how to interpret the information you got) and how to deal with other functionality of OSSEC (like FIM, file integrity and file meta data checks like tripwire or aide, rootkit detection, and so on). When you start with OSSEC you don't want to deal with the installer or where to get new binary releases or how to connect clients to the server. This book gives you a way around these important but time consuming tasks and will give you a running OSSEC installation on a server and clients which will provide some security out of the box. What I missed in this part is that you don't have to whitelist any client in your network but you can use OSSEC to detect if oneof your clients was compromised and lock this client out of all other clients.Since IDS systems have to be customized to your environment and due to the shortness of the book you will not find a complete manual on how to secure your entire network with OSSEC but it will give you a good starting point with the before mentioned decoders and rules by showing you an example upon which you can build your own configuration. Furthermore, you'll see how to enable extra features like rootkit detection which do not need much configuration and an example for an active response (intrusion countermeasures - blocking attacking hosts via iptables). The last part shows an advanced topic: helping OSSEC see the difference between a legitimate change to roots crontab via puppet and changes made by an attacker. This part shows that you can use OSSEC to gather information from different sources so can use it to aggregate information not only from standard OS logfiles but from very different sources of data like other security tools like fail2ban, Snort and many more so you can take action on your clients to based information from a vast amount of data.What I miss is a part about the agent configuration that you can change on your server which get's sent to your clients. Especially about what information has to be added to the server configuration and what should be sent to the clients. It could show another great feature of OSSEC: You can define global configuration options as well as options just for some clients (e.g. OS based) on the server and the client executes only the applicable config.The book is very short and it will not make you an IT security expert but it will give you a working OSSEC instance with a server and clients so you can test it and it will give you a good base to start yourself-studies.I enjoyed reading this book and I found some new information. Especially about a new way to connect your clients to your server and the part about checking whether a change was made by puppet or an attacker. I will definitely use it as a quick reference when setting up a new OSSEC HIDS infrastructure. I tried some of the examples from the book and the rest is at least very similar to what I do on my own OSSEC installation (although I would not recommend piping a script via wget to sh but download the installer script, check and run it. Just a small hint I could not resist to give).

KurzbeschreibungIn DetailSecurity 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.ApproachFilled 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 forThis 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 youre new to OSSEC-HIDS or a seasoned veteran, youll find something in this book you can apply today!This book assumes some knowledge of basic security concepts and rudimentary scripting experience.KurzbeschreibungIn DetailSecurity 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.ApproachFilled 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 forThis 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 youre new to OSSEC-HIDS or a seasoned veteran, youll find something in this book you can apply today!This book assumes some knowledge of basic security concepts and rudimentary scripting experience.ber den Autor und weitere MitwirkendeBrad 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!