Security Log Management: Identifying Patterns in the Chaos

Jacob Babbin

Security Log Management: Identifying Patterns in the Chaos

Jacob Babbin

Security Log Management: Identifying Patterns in the Chaos Jacob Babbin
This book teaches IT professionals how to analyze, manage, and automate their security log files to generate useful, repeatable information that can be use to make their networks more efficient and secure using primarily open source tools. The book begins by discussing the “Top 10” security logs that every IT professional should be regularly analyzing. These 10 logs cover everything from the top workstations sending/receiving data through a firewall to the top targets of IDS alerts. The book then goes on to discuss the relevancy of all of this information. Next, the book describes how to script open source reporting tools like Tcpdstats to automatically correlate log files from the various network devices to the “Top 10” list. By doing so, the IT professional is instantly made aware of any critical vulnerabilities or serious degradation of network performance. All of the scripts presented within the book will be available for download from the Syngress Solutions Web site.

Almost every operating system, firewall, router, switch, intrusion detection system, mail server, Web server, and database produces some type of “log file.” This is true of both open source tools and commercial software and hardware from every IT manufacturer. Each of these logs is reviewed and analyzed by a system administrator or security professional responsible for that particular piece of hardware or software. As a result, almost everyone involved in the IT industry works with log files in some capacity.

* Provides turn-key, inexpensive, open source solutions for system administrators to analyze and evaluate the overall performance and security of their network
* Dozens of working scripts and tools presented throughout the book are available for download from Syngress Solutions Web site.
* Will save system administrators countless hours by scripting and automating the most common to the most complex log analysis tasks

Download and Read Free Online Security Log Management: Identifying Patterns in the Chaos Jacob Babbin

From reader reviews:

Paul Blecha:

In other case, little persons like to read book Security Log Management: Identifying Patterns in the Chaos. You can choose the best book if you want reading a book. So long as we know about how is important any book Security Log Management: Identifying Patterns in the Chaos. You can add information and of course you can around the world by the book. Absolutely right, simply because from book you can realize everything! From your country till foreign or abroad you can be known. About simple point until wonderful thing you may know that. In this era, we can open a book or searching by internet gadget. It is called e-book. You should use it when you feel bored to go to the library. Let's read.

Floyd Hatfield:

Book will be written, printed, or created for everything. You can understand everything you want by a reserve. Book has a different type. To be sure that book is important thing to bring us around the world. Close to that you can your reading talent was fluently. A reserve Security Log Management: Identifying Patterns in the Chaos will make you to be smarter. You can feel considerably more confidence if you can know about every thing. But some of you think in which open or reading some sort of book make you bored. It is not necessarily make you fun. Why they can be thought like that? Have you in search of best book or ideal book with you?

Garnet Veach:

Do you among people who can't read pleasurable if the sentence chained from the straightway, hold on guys this aren't like that. This Security Log Management: Identifying Patterns in the Chaos book is readable by means of you who hate the straight word style. You will find the details here are arrange for enjoyable reading experience without leaving even decrease the knowledge that want to offer to you. The writer of Security Log Management: Identifying Patterns in the Chaos content conveys the idea easily to understand by most people. The printed and e-book are not different in the information but it just different as it. So , do you nevertheless thinking Security Log Management: Identifying Patterns in the Chaos is not loveable to be your top listing reading book?

Joe Garner:

The actual book Security Log Management: Identifying Patterns in the Chaos will bring you to the new experience of reading some sort of book. The author style to explain the idea is very unique. If you try to find new book to read, this book very appropriate to you. The book Security Log Management: Identifying Patterns in the Chaos is much recommended to you to study. You can also get the e-book from official web site, so you can quickly to read the book.

Download and Read Online Security Log Management: Identifying Patterns in the Chaos Jacob Babbin #TEKCSFM0U82

Read Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin for online ebook

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin 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 Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin books to read online.

Online Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin ebook PDF download

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin Doc

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin Mobipocket

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin EPub