Security Log Management: Identifying Patterns in the Chaos

Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez

Security Log Management: Identifying Patterns in the Chaos

Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez

Security Log Management: Identifying Patterns in the Chaos Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez
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, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez

---

From reader reviews:

Vivian Bennett:

You are able to spend your free time you just read this book this publication. This Security Log Management: Identifying Patterns in the Chaos is simple to create you can read it in the area, in the beach, train and also soon. If you did not possess much space to bring typically the printed book, you can buy the actual e-book. It is make you easier to read it. You can save the book in your smart phone. Thus there are a lot of benefits that you will get when one buys this book.

Robert Aviles:

Many people spending their moment by playing outside together with friends, fun activity using family or just watching TV all day every day. You can have new activity to pay your whole day by reading through a book. Ugh, think reading a book really can hard because you have to take the book everywhere? It okay you can have the e-book, taking everywhere you want in your Mobile phone. Like Security Log Management: Identifying Patterns in the Chaos which is having the e-book version. So , why not try out this book? Let's view.

Albert Chesson:

Is it anyone who having spare time then spend it whole day by means of watching television programs or just telling lies on the bed? Do you need something new? This Security Log Management: Identifying Patterns in the Chaos can be the solution, oh how comes? A book you know. You are consequently out of date, spending your spare time by reading in this fresh era is common not a nerd activity. So what these textbooks have than the others?

Harry Baxter:

A lot of people said that they feel fed up when they reading a e-book. They are directly felt that when they get a half elements of the book. You can choose the particular book Security Log Management: Identifying Patterns in the Chaos to make your own reading is interesting. Your own personal skill of reading proficiency is developing when you just like reading. Try to choose very simple book to make you enjoy to study it and mingle the feeling about book and reading especially. It is to be first opinion for you to like to open up a book and study it. Beside that the publication Security Log Management: Identifying Patterns in the Chaos can to be your brand new friend when you're sense alone and confuse in doing what must you're doing of that time.

Read Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez for online ebook

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez 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, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez books to read online.

Online Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez ebook PDF download

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez Doc

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez Mobipocket

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez EPub

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez Ebook online

Security Log Management: Identifying Patterns in the Chaos by Jacob Babbin, Dave Kleiman, Everett F. Carter Jr., Jeremy Faircloth, Mark Burnett, Esteban Gutierrez Ebook PDF