Snort Intrusion Detection and Prevention Toolkit

Brian Caswell, Jay Beale, Andrew Baker

Snort Intrusion Detection and Prevention Toolkit

Brian Caswell, Jay Beale, Andrew Baker

Snort Intrusion Detection and Prevention Toolkit Brian Caswell, Jay Beale, Andrew Baker
This all new book covering the brand new Snort version 2.6 from members of the Snort developers team.

This fully integrated book and Web toolkit covers everything from packet inspection to optimizing Snort for speed to using the most advanced features of Snort to defend even the largest and most congested enterprise networks. Leading Snort experts Brian Caswell, Andrew Baker, and Jay Beale analyze traffic from real attacks to demonstrate the best practices for implementing the most powerful Snort features.

The companion material contains examples from real attacks allowing readers test their new skills. The book will begin with a discussion of packet inspection and the progression from intrusion detection to intrusion prevention. The authors provide examples of packet inspection methods including: protocol standards compliance, protocol anomaly detection, application control, and signature matching. In addition, application-level vulnerabilities including Binary Code in HTTP headers, HTTP/HTTPS Tunneling, URL Directory Traversal, Cross-Site Scripting, and SQL Injection will also be analyzed. Next, a brief chapter on installing and configuring Snort will highlight various methods for fine tuning your installation to optimize Snort performance including hardware/OS selection, finding and eliminating bottlenecks, and benchmarking and testing your deployment. A special chapter also details how to use Barnyard to improve the overall performance of Snort. Next, best practices will be presented allowing readers to enhance the performance of Snort for even the largest and most complex networks. The next chapter reveals the inner workings of Snort by analyzing the source code. The next several chapters will detail how to write, modify, and fine-tune basic to advanced rules and pre-processors. Detailed analysis of real packet captures will be provided both in the book and the companion material. Several examples for optimizing output plugins will then be discussed including a comparison of MySQL and PostrgreSQL. Best practices for monitoring Snort sensors and analyzing intrusion data follow with examples of real world attacks using: ACID, BASE, SGUIL, SnortSnarf, Snort_stat.pl, Swatch, and more.

The last part of the book contains several chapters on active response, intrusion prevention, and using Snort's most advanced capabilities for everything from forensics and incident handling to building and analyzing honey pots. Data from real world attacks will be presented throughout this part as well as on the companion website, http://booksite.elsevier.com/9781597490993/

- This fully integrated book and Web toolkit covers everything all in one convenient package
- It is authored by members of the Snort team and it is packed full of their experience and expertise
- Includes full coverage of the brand new Snort version 2.6, packed full of all the latest information
- Companion website at http://booksite.elsevier.com/9781597490993/ contains all companion material

Download and Read Free Online Snort Intrusion Detection and Prevention Toolkit Brian Caswell, Jay Beale, Andrew Baker

From reader reviews:

Terry Smith:

Inside other case, little folks like to read book Snort Intrusion Detection and Prevention Toolkit. You can choose the best book if you appreciate reading a book. As long as we know about how is important a book Snort Intrusion Detection and Prevention Toolkit. You can add knowledge and of course you can around the world by a book. Absolutely right, due to the fact from book you can recognize everything! From your country right up until foreign or abroad you will end up known. About simple issue until wonderful thing you can know that. In this era, we can open a book or even searching by internet device. It is called e-book. You may use it when you feel bored stiff to go to the library. Let's study.

Karen Taylor:

The book Snort Intrusion Detection and Prevention Toolkit gives you the sense of being enjoy for your spare time. You should use to make your capable more increase. Book can being your best friend when you getting tension or having big problem with your subject. If you can make reading a book Snort Intrusion Detection and Prevention Toolkit for being your habit, you can get much more advantages, like add your capable, increase your knowledge about several or all subjects. You may know everything if you like available and read a book Snort Intrusion Detection and Prevention Toolkit. Kinds of book are several. It means that, science reserve or encyclopedia or other folks. So , how do you think about this publication?

Paul Jackson:

Hey guys, do you would like to finds a new book to learn? May be the book with the title Snort Intrusion Detection and Prevention Toolkit suitable to you? The actual book was written by well known writer in this era. The actual book untitled Snort Intrusion Detection and Prevention Toolkitis the main of several books this everyone read now. This specific book was inspired a number of people in the world. When you read this e-book you will enter the new dimension that you ever know ahead of. The author explained their strategy in the simple way, so all of people can easily to know the core of this publication. This book will give you a wide range of information about this world now. To help you to see the represented of the world with this book.

Dolores Albert:

Reading a e-book can be one of a lot of activity that everyone in the world loves. Do you like reading book consequently. There are a lot of reasons why people enjoyed. First reading a book will give you a lot of new facts. When you read a e-book you will get new information due to the fact book is one of several ways to share the information or maybe their idea. Second, examining a book will make a person more imaginative. When you reading through a book especially tale fantasy book the author will bring that you imagine the story how the character types do it anything. Third, you can share your knowledge to other people. When you read this Snort Intrusion Detection and Prevention Toolkit, it is possible to tells your family, friends and also soon about yours publication. Your knowledge can inspire others, make them reading a reserve.

Download and Read Online Snort Intrusion Detection and Prevention Toolkit Brian Caswell, Jay Beale, Andrew Baker #N6CE2ZTS9WQ

Read Snort Intrusion Detection and Prevention Toolkit by Brian Caswell, Jay Beale, Andrew Baker for online ebook

Snort Intrusion Detection and Prevention Toolkit by Brian Caswell, Jay Beale, Andrew Baker 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 Snort Intrusion Detection and Prevention Toolkit by Brian Caswell, Jay Beale, Andrew Baker books to read online.

Online Snort Intrusion Detection and Prevention Toolkit by Brian Caswell, Jay Beale, Andrew Baker ebook PDF download

Snort Intrusion Detection and Prevention Toolkit by Brian Caswell, Jay Beale, Andrew Baker Doc

Snort Intrusion Detection and Prevention Toolkit by Brian Caswell, Jay Beale, Andrew Baker Mobipocket

Snort Intrusion Detection and Prevention Toolkit by Brian Caswell, Jay Beale, Andrew Baker EPub