Review of the book

"Introduction to Security and Network Forensics"

by William J. Buchanan

CRC Press, Taylor & Francis Group, 2011

ISBN: 978-0-8493-3568-6

S. V. Nagaraj
RMK Engineering College

2012-04-15

1 Summary of the review

This review is about a book that offers an introduction to security and network forensics. It focuses on the basics of concepts such as intrusion detection systems, authentication, encryption, and network forensics. The book has twelve chapters.

2 Summary of the book

The book is an introductory text that contains information about intrusion detection systems, encryption, authentication, hashing, digital signatures, enhanced software security, network security elements, risk, threat analysis, network forensics, data hiding and obfuscation, Web infrastructures, and cloud/grid computing. It is made up of twelve chapters.

Chapter 1 (Introduction to Security) offers a brief overview of some important terms used in security. It introduces concepts such as defense-in-depth and demilitarized zones.

Chapter 2 (Intrusion Detection Systems) looks at intrusions, attack patterns, and systems such as Snort for intrusion detection. Typical detection procedures are discussed.

Chapter 3 (Encryption) studies the basics of encryption, public key and private key encryption. It discussers several methods for encryption and ways of deciphering encrypted content.

Chapter 4 (Authentication, Hashing, and Digital Certificates) describes some methods for authentication. The concepts made clear include digital certificates and Public Key Infrastructure. Hash functions and their applications are also highlighted. The Kerberos system for authentication is introduced along with email encryption.

Chapter 5 (Enhanced Software Security) explains some of the security concepts employed in the Microsoft .NET environment. This provides an illustration into how security is integrated into applications.

Chapter 6 (Network Security Elements) provides a brief overview of network security elements such as routers, proxy servers and firewalls. The application of Network Address Translation (NAT) is also mentioned.

Chapter 7 (Introduction to Risk) brings in the concept of risk. Various types of threats to systems are highlighted. The notion of service-oriented infrastructures is introduced with reference to Linux and

Windows operating systems. A brief overview of services, logging, and auditing with these operating systems is given.

Chapter 8 (Threat Analysis) familiarizes the approach an intruder might take during an intrusion. An introduction to vulnerability analysis and vulnerability scanners is provided.

Chapter 9 (Network Forensics) discusses key network protocols such as IP, TCP, ARP, and ICMP. The methodologies used in network forensics and the sources for network activity are also covered.

Chapter 10 (Data Hiding and Obfuscation) highlights some methods for obfuscation. These methods make use of encryption and tunnelling. Covert channels, watermarking, and steganography are also studied. Methods for hiding the contents of files are also discussed.

Chapter 11 (Web Infrastructures) looks at Web-based infrastructures in the context of authentication and access control. Protocols such as Kerberos and SOAP are introduced. Emphasis is placed on scalability and extensibility.

Chapter 12 (Cloud/Grid Computing) is the final chapter of the book. It provides a basic overview of cluster, grid, and cloud infrastructures. An example that uses cloud-based infrastructure is demonstrated.

3 What is the book like (style)?

The book makes an interesting reading. The textbook is supplemented by online materials including lab exercises, online exercises, reference text, Cisco challenges, test questions, and videos. It is well written and highly readable. It places great emphasis on hands on learning as it includes plenty of ready made code that could be tried out. The chapters have tutorials and references for further exploration. This book is well suited for teaching beginners, undergrads, master's and doctoral level students. The problems and exercises at the end of each chapter will help the readers to test their comprehension. The book is well organized and the coverage of topics is excellent for an introductory text.

The most disappointing aspect of the book is the absence of page numbers. Page numbering is done only at the beginning of chapters. The index is useful and the items in the index do have page numbers, however, in the absence of page numbering in the main text, it is very difficult to discover in which page the indexed material lies. Most pages have some huge avoidable empty space. This may help readability but unfortunately it increases the size of the book. Most of the diagrams in the book employ small fonts, and consequently readability becomes a big issue. The empty space in the pages could have been used to produce more readable diagrams and illustrations. The key positive aspect of the book is the provision of several exercises at the end of the chapters. They are very interesting and reinforce the learning of the reader. It should be said that there are numerous introductory books on security in the market, however, this book is very unique due to its emphasis on clarity and hands on learning supplemented by exercises.

4 Would you recommend this book?

This book offers an excellent practical introduction to important issues concerning network security and forensics. It will be a boon for novices, students and researchers. I strongly recommend this book as a useful introductory text on network security.

The reviewer is a Professor at the CSE Dept., RMK Engg. College, Kavaraipettai, Tamil Nadu, India