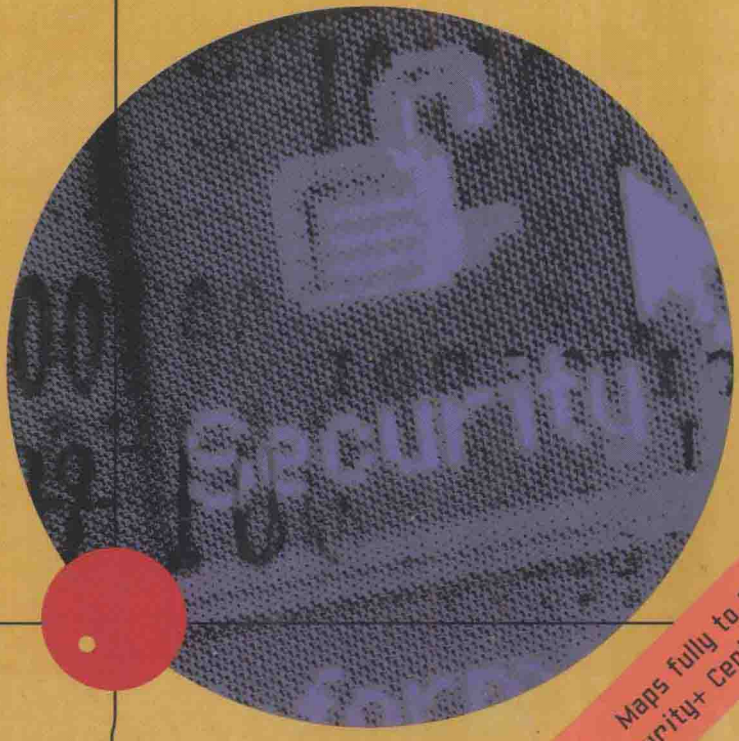
THOMSON
COURSE TECHNOLOGY

SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS

CISCO LEARNING INSTITUTE

PAUL CAMPBELL, BEN CALVERT, STEVEN BOSWELL



CompTIA Authorized Quality Curriculum

PREPARING TOMORROW'S INFORMATION SECURITY PROFESSIONALS

CompTIA. Security+™ Certification Program

Maps fully to CompTIA's Security+ Certification Exam

Security+ Guide to Network Security Fundamentals

By Cisco Learning Institute

Paul Campbell
Ben Calvert
Steven Boswell

THOMSON
COURSE TECHNOLOGY

Australia • Canada • Mexico • Singapore • Spain • United Kingdom • United States

Security+ Guide to Network Security Fundamentals

By Cisco Learning Institute

Paul Campbell
Ben Calvert
Steven Boswell

Senior Editor:
William Pitkin III

Product Manager:
Laura Hildebrand

Production Editor:
Brooke Booth

Technical Reviewers:
Mark Weiser, Eileen Vidrine, Dave DiFabio, Mike Nicholas, Rob Andrews

Manuscript Quality Assurance Manager:
John Bosco

MQA Technical Lead:
Nicole Ashton

MQA Testers:
Christian Kunciw, Chris Scriver

Associate Product Manager:
Tim Gleeson

Editorial Assistant:
Nick Lombardi

Marketing Manager:
Jason Sakos

Text Designer:
GEX Publishing Services

Compositor:
GEX Publishing Services

Cover Design:
Janet Lavine

Printed in Canada

1 2 3 4 5 6 7 8 9 WC 06 05 04 03

For more information, contact Course Technology, 25 Thomson Place, Boston, Massachusetts, 02210.

Or find us on the World Wide Web at: www.course.com

ISBN 0-619-12017-7

Preface

At one time not so long ago, the only computer security necessary was a locked door to protect a huge mainframe from vandals or thieves. In the "old days" the only way to compromise data stored in a computer was to get into the computer room and manually alter the data through the computer's terminal. Desktop computers and the advent of networking put the power of a computer and access to a company's data in the hands of every employee. While this evolution has increased productivity worldwide, it has also given birth to a whole new field of network security. As networks have developed and become more sophisticated, so have the techniques available to the unscrupulous individuals who invade an organization's private space and do damage or take advantage of the critical data that resides there. *Security+ Guide to Network Security Fundamentals* takes a comprehensive look at network security and provides instructors and students with an organized view of the field, and the tools and techniques necessary to safeguard one of corporate America's most significant assets—its computer stored data.

This book offers in-depth coverage of all the current risks and threats to an organization's data along with a structured way of addressing the safeguarding of these critical electronic assets. The book provides the theoretical and historical background necessary to understand the various types of risks as well as the hands on, practical techniques for working in the security field in the twenty-first century. The events of September 2001 have further driven home the need for a secure environment and whenever possible, we have addressed the need for heightened security to protect corporate and governmental resources from the deeds of professional criminals and terrorists.

The Intended Audience

This book is intended to serve the needs of individuals interested in understanding the field of network security and how the field relates to other areas of Information Technology. The material in this book will provide the broad-based knowledge necessary to prepare students for further study in specialized security fields or may be used as a capstone course to those interested in a general introduction to the field. This book is also intended to serve the needs of individuals seeking to pass the Computing Technology Industry Association's Security+ certification exam. For more information on Security+ certification, visit CompTIA's web site at *www.comptia.org*.

The authors assume that students using this book have an understanding of computer networking and basic router configuration.

between host-based and network-based systems are covered as well as active and passive detection features. Honeypots, and their use in increasing network security, along with the role of security incident response teams are also covered.

Chapter 13 A complete understanding of security baselines is essential to understanding network security. This chapter provides a good understanding of Operating System vulnerabilities and OS hardening practices. Common network services that are often exploited by hackers are covered along with practices for securing a file system and network hardening practices.

Chapter 14 presents the basics of algorithms and how they are used in modern cryptography. The differences between asymmetric and symmetric algorithms are covered. The basics of cryptography are covered, including the characteristics of PKI certificates and the policies and procedures surrounding them.

Chapter 15 discusses the importance of physical security, a basic but critical part of network security easily overlooked. This chapter underscores the importance of where data storage systems are located within an organization, and includes major considerations when building or selecting a site. Biometrics is discussed along with the importance of fire safety and fire detection.

Chapter 16 outlines the critical and rather complicated process of disaster recovery planning along with the process and procedures that an organization should employ.

Chapter 17 The advent of computer and network fraud has created a new field of network security forensics. This field centers on the rules of evidence governing the detection and prosecution of network-related damage and crime. This chapter deals with risk identification, education and documentation.

Features

To ensure a successful learning experience, this book includes the following pedagogical features:

- **Chapter Objectives:** Each chapter in this book begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with a quick reference to the contents of that chapter, as well as a useful study aid.
- **Illustrations and Tables:** Where applicable, illustrations, photographs, and tables are provided to further aid you in your understanding of security concepts.
- **End-of-Chapter Material:** The end of each chapter includes the following features to reinforce the material covered in the chapter:
  - **Chapter Summary:** Gives a brief but complete summary of the chapter
  - **Key Terms List:** Lists all new terms and their definitions

- **Review Questions:** Test your knowledge of the most important concepts covered in the chapter
- 

Hands-on Projects: Help you to apply the knowledge gained in the chapter
- 

Security Projects: Provide additional scenario- or research-based exercises to further reinforce the concepts presented

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand what is being discussed in the chapter. Icons throughout the text alert you to additional materials. The icons used in this textbook are as follows:

Tips are included from the authors' experiences that provide additional real-world insights into the topic being discussed.

Notes are used to present additional helpful material related to the subject being described and may direct the reader to another location in the book where a certain topic is covered.

Hands-on Projects are preceded by the Hands-on icon and a description of the exercise that follows.

Security Project icons mark the exercises in the book that are either scenario-based or research-based.

Instructor's Materials

The following supplemental materials are available when this book is used in a classroom setting. All of the supplements available with this book are provided to the instructor on a single CD-ROM.

Electronic Instructor's Manual: The Instructor's Manual that accompanies this textbook includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.

Solutions: Answers to all end-of-chapter materials, including the Review Questions, and, when applicable, Hands-on Projects, and Security Projects.

ExamView®: This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this text, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers, and also save the instructor time by grading each exam automatically.

PowerPoint presentations: This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.

Figure Files: All of the figures in the book are reproduced on the Instructor's Resource CD in bit-mapped format. Similar to the PowerPoint presentations, these are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

MeasureUp™ Test Prep Software: Test preparation software for the Security+ exam will be available within 120 days of the final exam's release. You can download copies of this software free of charge at Course Technology's website at: *www.course.com/security*. Click the link for Security+ Test Prep. The user name and password is: testprep. This password is case sensitive and does not contain a space between the two words.

ACKNOWLEDGMENTS

The authors would like to thank Course Technology for their support during the development of this book. We deeply appreciate their patience and indulgence, especially that of Steven Elliot, Associate Publisher; Will Pitkin, Senior Editor; and Laura Hildebrand, our Product Manager. We would also like to thank our Production Editor, Brooke Booth, for keeping this project on track. Special thanks to our Technical Editor, Mark Weiser, and MQA Testers Christian Kunciw and Chris Scriver, for identifying technical errors, and the reviewers, Eileen Vidrine, Dave DiFabio, Rob Andrews, and Mike Nicholas for their helpful criticisms and comments.

The Cisco Learning Institute (CLI) developed this book, and the companion interactive course available separately on CD-ROM. The Institute is a 501 C3 not-for-profit public benefit corporation dedicated to enhancing the way teachers teach and students learn using technology. The Institute provides continuing assistance, software, and support of the curriculum that is delivered as part of the Cisco Networking Academy Program, the largest e-learning deployment in the world.

For more information about the Cisco Learning Institute or for information on how the Institute can help you with your e-learning deployment needs, visit *www.ciscolearning.org*. The Institute would like to thank the authors for their diligent effort to produce this product, and Course Technology for their valuable help as an educational partner.

Paul Campbell

While developing my chapters for this book, I discovered firsthand that actually writing about a subject for publication is much, much more demanding than simply speaking about it. I would like to thank all of the editors, who provided sound technical and other advice to enable my chapters to flow more smoothly and accurately, as well as all of the other people who helped publish this book. I would also like to extend my deepest gratitude to my family and friends for all the support and encouragement they provided during this project and indeed, throughout my entire life.

Ben Calvert

I'd like to acknowledge my wife, Shahnoza, for her incredible support during the long days and nights that were required to write this book. Thanks to my mom for an upbringing that got me to where I am today, making this book a possibility for me. Finally, thanks to my co-authors and friends who have made it all worthwhile.

Steven Boswell

I would like to thank my friends and family for offering their encouragement and support while I was writing this book. I would also like to thank Ben and Paul for their hard work and dedication to this project. Thanks guys! And finally, I would like to thank Larisa, my wife, for her love and continual encouragement that has enabled me to accomplish things I never thought were possible.

Photo Credits

Figure 2-7	Courtesy of DigitalPersona, Inc.
Figure 2-8	Courtesy of Human Recognition Systems (UK) Ltd.
Figure 2-9	Courtesy of Retinal Technologies, Inc.
Figure 2-10	Courtesy of Panasonic
Figure 2-11	Courtesy of Interlink Electronics, Inc.
Figure 8-1	Courtesy of SANYO Fisher Company
Figure 8-2	Courtesy of Handspring
Figure 8-6	Courtesy of 3Com Corporation
Figure 8-7	Courtesy of NETGEAR
Figure 9-4	Courtesy of 3Com Corporation
Figure 9-6	EtherFast® Cable Modem with USB and Ethernet Connection Model BEFCMU10 Courtesy of Linksys Group Inc.
Figure 9-11	T-Mobile Pocket PC Phone Edition Courtesy of T-Mobile International

Read This Before You Begin

To the User

This book should be read in sequence, from beginning to end. Each chapter builds upon those that precede it to provide a solid understanding of networking security fundamentals. The book may also be used to prepare for CompTIA's Security + certification exam. The grid on the inside front cover of the book pinpoints the exact chapter in which a specific Security+ exam objective is located.

Readers are also encouraged to investigate the many pointers to online and printed sources of additional information that are cited throughout this book.

Security+ Interactive Course on CD-ROM

In addition to this text, CLI also developed the companion *Security+ Guide to Network Security Fundamentals Interactive Course on CD-ROM.* Available separately, this course parallels the book and greatly enhances the student's learning experience with interactive quizzes and illustrative simulations. The course is extremely flexible and can be run on nearly any modern computer, or loaded onto an institution's server for local access by students. The course was also designed to work with the most popular learning management systems, such as Blackboard or WebCT, for those interested in using the content as part of a distance learning offering. Regardless of how it is used, the *Security+ Guide to Network Security Fundamentals Interactive Course on CD-ROM* provides a level of interactivity that the book alone cannot provide, and creates a dynamic learning environment for the student. For more information please visit *www.course.com/security*.

Hardware and Software Requirements

Following are the hardware and software requirements needed to perform the end-of-chapter Hands-on Projects. All projects may be completed on a stand-alone computer with the exception of Projects 4-2 and 4-3, which require two PCs connected to a hub.

- Windows 2000 Server or Windows 2000 Professional operating system
- Outlook Express 6.0
- An Internet connection and Web browser (i.e. Internet Explorer)
- FTP client (will vary per computer)
- Hotmail account

For more information about the Cisco Learning Institute or for information on how the Institute can help you with your e-learning deployment needs, visit *www.ciscolearning.org*. The Institute would like to thank the authors for their diligent effort to produce this product, and Course Technology for their valuable help as an educational partner.

Paul Campbell

While developing my chapters for this book, I discovered firsthand that actually writing about a subject for publication is much, much more demanding than simply speaking about it. I would like to thank all of the editors, who provided sound technical and other advice to enable my chapters to flow more smoothly and accurately, as well as all of the other people who helped publish this book. I would also like to extend my deepest gratitude to my family and friends for all the support and encouragement they provided during this project and indeed, throughout my entire life.

Ben Calvert

I'd like to acknowledge my wife, Shahnoza, for her incredible support during the long days and nights that were required to write this book. Thanks to my mom for an upbringing that got me to where I am today, making this book a possibility for me. Finally, thanks to my co-authors and friends who have made it all worthwhile.

Steven Boswell

I would like to thank my friends and family for offering their encouragement and support while I was writing this book. I would also like to thank Ben and Paul for their hard work and dedication to this project. Thanks guys! And finally, I would like to thank Larisa, my wife, for her love and continual encouragement that has enabled me to accomplish things I never thought were possible.

Photo Credits

Figure 2-7	Courtesy of DigitalPersona, Inc.
Figure 2-8	Courtesy of Human Recognition Systems (UK) Ltd.
Figure 2-9	Courtesy of Retinal Technologies, Inc.
Figure 2-10	Courtesy of Panasonic
Figure 2-11	Courtesy of Interlink Electronics, Inc.
Figure 8-1	Courtesy of SANYO Fisher Company
Figure 8-2	Courtesy of Handspring
Figure 8-6	Courtesy of 3Com Corporation
Figure 8-7	Courtesy of NETGEAR
Figure 9-4	Courtesy of 3Com Corporation
Figure 9-6	EtherFast® Cable Modem with USB and Ethernet Connection Model BEFCMU10 Courtesy of Linksys Group Inc.
Figure 9-11	T-Mobile Pocket PC Phone Edition Courtesy of T-Mobile International

Specialized Requirements

Whenever possible, the need for specialized requirements were kept to a minimum. The following chapters feature specialized hardware/software:

- Chapter 8: a notebook computer, a wireless NIC, and a Cisco Aironet access point or 3Com AirConnect access point
- Chapter 7, Hands-on Project 7-5: Netscape 7.0
- Chapter 11: diagramming software

Free Downloadable Software is required in the following chapters:

Chapter 3:

- Cerberus Internet Scanner (CIS)
- Foundstone's FPort and SuperScan 3.0 Trial Version
- PWDump 3.0
- John the Ripper

Chapter 5:

- Pretty Good Privacy (PGP) 7.0

Chapter 6:

- WinPcap 3.0
- Ethereal

Chapter 7:

- Legion 2.1

Chapter 9:

- Zone Alarm

Chapter 10:

- Packet analyzer of choice

Chapter 12:

- BackOfficer Friendly
- Foundstone's SuperScan 3.0 Trial Version

Chapter 13:

- LC4 Trial Version
- Sniff'em

Chapter 14:

- Fingerprint Synthesis
- VeriFinger 4.0 Evaluation Version

TABLE OF

Contents