## Brief Contents

### INTRODUCTION xiii

| CHAPTER 1 | Introduction to Security | 1 |

**Security+ Domain 1.0: Systems Security**

| CHAPTER 2 | Systems Threats and Risks | 39 |
| CHAPTER 3 | Protecting Systems | 79 |

**Security+ Domain 2.0: Network Infrastructure**

| CHAPTER 4 | Network Vulnerabilities and Attacks | 119 |
| CHAPTER 5 | Network Defenses | 153 |
| CHAPTER 6 | Wireless Network Security | 189 |

**Security+ Domain 3.0: Access Control**

| CHAPTER 7 | Access Control Fundamentals | 225 |
| CHAPTER 8 | Authentication | 265 |

**Security+ Domain 4.0: Assessments & Audits**

| CHAPTER 9 | Performing Vulnerability Assessments | 301 |
| CHAPTER 10 | Conducting Security Audits | 331 |

**Security+ Domain 5.0: Cryptography**

| CHAPTER 11 | Basic Cryptography | 365 |
| CHAPTER 12 | Applying Cryptography | 399 |

**Security+ Domain 6.0: Organizational Security**

| CHAPTER 13 | Business Continuity | 439 |
| CHAPTER 14 | Security Policies and Training | 477 |
# Table of Contents

## INTRODUCTION

### CHAPTER 1

**Introduction to Security**

- Challenges of Securing Information  
  - Today’s Security Attacks  
  - Difficulties in Defending against Attacks  
- What Is Information Security?  
  - Defining Information Security  
  - Information Security Terminology  
  - Understanding the Importance of Information Security  
- Who Are the Attackers?  
  - Hackers  
  - Script Kiddies  
  - Spies  
  - Employees  
  - Cybercriminals  
  - Cyberterrorists  
- Attacks and Defenses  
  - Steps of an Attack  
  - Defenses against Attacks  
  - Layering  
  - Limiting  
  - Diversity  
  - Obscurity  
  - Simplicity  
- Surveying Information Security Careers and the Security+ Certification  
  - Types of Information Security Jobs  
  - CompTIA Security+ Certification  
- Chapter Summary  
- Key Terms  
- Review Questions  
- Hands-on Projects  
- Case Projects  

### CHAPTER 2

**Systems Threats and Risks**

- Software-Based Attacks  
  - Infecting Malware  
  - Concealing Malware  
  - Malware for Profit  
- Hardware-Based Attacks  
  - BIOS  
  - USB Devices  
  - Network Attached Storage (NAS)  
  - Cell Phones  
- Attacks on Virtualized Systems  
  - What Is Virtualization?  
  - Attacks on Virtual Systems  

---

1. Challenges of Securing Information  
2. Today’s Security Attacks  
3. Difficulties in Defending against Attacks  
4. What Is Information Security?  
5. Defining Information Security  
6. Information Security Terminology  
7. Understanding the Importance of Information Security  
8. Who Are the Attackers?  
9. Hackers  
10. Script Kiddies  
11. Spies  
12. Employees  
13. Cybercriminals  
14. Cyberterrorists  
15. Attacks and Defenses  
16. Steps of an Attack  
17. Defenses against Attacks  
18. Layering  
19. Limiting  
20. Diversity  
21. Obscurity  
22. Simplicity  
24. Types of Information Security Jobs  
25. CompTIA Security+ Certification  
26. Chapter Summary  
27. Key Terms  
28. Review Questions  
29. Hands-on Projects  
30. Case Projects  
31. Software-Based Attacks  
32. Infecting Malware  
33. Concealing Malware  
34. Malware for Profit  
35. Hardware-Based Attacks  
36. BIOS  
37. USB Devices  
38. Network Attached Storage (NAS)  
39. Cell Phones  
40. Attacks on Virtualized Systems  
41. What Is Virtualization?  
42. Attacks on Virtual Systems  

---

v
## Table of Contents

- **Chapter Summary** 63  
- **Key Terms** 64  
- **Review Questions** 67  
- **Hands-on Projects** 70  
- **Case Projects** 76  

### CHAPTER 3  
**Protecting Systems** 79

- **Hardening the Operating System** 81  
  - Managing Operating System Updates 81  
  - Buffer Overflow Protection 85  
  - Configuring Operating System Protection 88  
- **Preventing Attacks that Target the Web Browser** 89  
  - Cookies 89  
  - JavaScript 90  
  - Java 91  
  - ActiveX 92  
  - Cross Site Scripting (XSS) 93  
- **Hardening Web Servers** 95  
- **Protecting Systems from Communications-Based Attacks** 97  
  - SMTP Open Relays 97  
  - Instant Messaging 98  
  - Peer-to-Peer (P2P) Networks 99  
- **Applying Software Security Applications** 100  
  - Antivirus 100  
  - Popup Blockers 100  
  - Anti-Spam 101  
  - Personal Software Firewalls 103  
  - Host Intrusion Detection Systems (HIDS) 103  
- **Chapter Summary** 104  
- **Key Terms** 105  
- **Review Questions** 107  
- **Hands-on Projects** 110  
- **Case Projects** 117  

### CHAPTER 4  
**Network Vulnerabilities and Attacks** 119

- **Network Vulnerabilities** 121  
  - Media-Based Vulnerabilities 121  
  - Network Device Vulnerabilities 123  
- **Categories of Attacks** 126  
  - Denial of Service (DoS) 126  
  - Spoofing 130  
  - Man-in-the-Middle 130  
  - Replay 131  
- **Methods of Network Attacks** 131  
  - Protocol-Based Attacks 131  
  - Wireless Attacks 137  
  - Other Attacks and Frauds 141
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter Summary</td>
<td>142</td>
</tr>
<tr>
<td>Key Terms</td>
<td>143</td>
</tr>
<tr>
<td>Review Questions</td>
<td>145</td>
</tr>
<tr>
<td>Hands-on Projects</td>
<td>148</td>
</tr>
<tr>
<td>Case Projects</td>
<td>151</td>
</tr>
</tbody>
</table>

## CHAPTER 5

**Network Defenses** 153

- Crafting a Secure Network 155
  - Security through Network Design 155
  - Security through Network Technologies 162

- Applying Network Security Devices 165
  - Firewall 166
  - Proxy Server 169
  - Honeypot 170
  - Network Intrusion Detection Systems (NIDS) 171

- Host and Network Intrusion Prevention Systems (HIPS/NIPS) 172

- Protocol Analyzers 173

- Internet Content Filters 174

- Integrated Network Security Hardware 174

- Chapter Summary 175

- Key Terms 176

- Review Questions 177

- Hands-on Projects 180

- Case Projects 186

## CHAPTER 6

**Wireless Network Security** 189

- IEEE 802.11 Wireless Security Protections 191
  - Controlling Access 192

- Vulnerabilities of IEEE 802.11 Security 198
  - Open System Authentication Vulnerabilities 198
  - MAC Address Filtering Weaknesses 200
  - WEP 200

- Personal Wireless Security 202
  - WPA Personal Security 202
  - WPA2 Personal Security 204

- Enterprise Wireless Security 206
  - IEEE 802.11i 206
  - WPA Enterprise Security 207
  - WPA2 Enterprise Security 209
  - Enterprise Wireless Security Devices 209

- Chapter Summary 214

- Key Terms 215

- Review Questions 216

- Hands-on Projects 219

- Case Projects 223
# Table of Contents

## CHAPTER 7
### Access Control Fundamentals
- What Is Access Control?  
  - 227
- Access Control Terminology  
  - 227
- Access Control Models  
  - 229
- Practices for Access Control  
  - 233
- Logical Access Control Methods  
  - 234
  - Access Control Lists (ACLs)  
  - 234
  - Group Policies  
  - 236
  - Account Restrictions  
  - 236
  - Passwords  
  - 238
- Physical Access Control  
  - 244
  - Computer Security  
  - 244
  - Door Security  
  - 245
  - Mantraps  
  - 248
  - Video Surveillance  
  - 249
  - Physical Access Log  
  - 249
- Chapter Summary  
  - 250
- Key Terms  
  - 251
- Review Questions  
  - 253
- Hands-on Projects  
  - 256
- Case Projects  
  - 263

## CHAPTER 8
### Authentication
- Definition of Authentication  
  - 267
  - Authentication and Access Control Terminology  
  - 267
  - Authentication, Authorization, and Accounting (AAA)  
  - 267
- Authentication Credentials  
  - 268
  - One-Time Passwords  
  - 268
  - Standard Biometrics  
  - 270
  - Behavioral Biometrics  
  - 271
  - Cognitive Biometrics  
  - 273
  - Authentication Models  
  - 275
  - Authentication Servers  
  - 278
  - RADIUS  
  - 278
  - Kerberos  
  - 280
  - Terminal Access Control Access Control System (TACACS+)  
  - 280
  - Lightweight Directory Access Protocol (LDAP)  
  - 281
- Extended Authentication Protocols (EAP)  
  - 282
  - Authentication Legacy Protocols  
  - 282
  - EAP Weak Protocols  
  - 283
  - EAP Strong Protocols  
  - 283
- Remote Authentication and Security  
  - 284
  - Remote Access Services (RAS)  
  - 284
  - Virtual Private Networks (VPNs)  
  - 284
  - Remote Access Policies  
  - 287
- Chapter Summary  
  - 287
- Key Terms  
  - 288
- Review Questions  
  - 291
# CHAPTER 12

## Applying Cryptography

**Digital Certificates**
- Defining Digital Certificates
- Authorizing, Storing, and Revoking Digital Certificates
- Types of Digital Certificates

**Public Key Infrastructure (PKI)**
- What Is Public Key Infrastructure (PKI)?
- Public-Key Cryptographic Standards (PKCS)
- Trust Models
- Managing PKI

**Key Management**
- Key Storage
- Key Usage
- Key Handling Procedures

**Cryptographic Transport Protocols**
- File Transfer Protocols
- Web Protocols
- VPN Protocols
- E-mail Transport Protocol

**Chapter Summary**

**Key Terms**

**Review Questions**

**Hands-on Projects**

**Case Projects**

---

# CHAPTER 13

## Business Continuity

**Environmental Controls**
- Fire Suppression
- Electromagnetic Shielding
- HVAC
# Table of Contents

Redundancy Planning 446
  - Servers 446
  - Storage 447
  - Networks 451
  - Power 451
  - Sites 452

Disaster Recovery Procedures 452
  - Planning 452
  - Disaster Exercises 455
  - Data Backups 455

Incident Response Procedures 459
  - What Is Forensics? 459
  - Responding to a Computer Forensics Incident 460

Chapter Summary 464
  - Key Terms 465
  - Review Questions 467
  - Hands-on Projects 470
  - Case Projects 475

CHAPTER 14
## Security Policies and Training 477

Organizational Security Policies 479
  - What Is a Security Policy? 479
  - Balancing Trust and Control 480
  - Designing a Security Policy 481

Types of Security Policies 485
  - Acceptable Use Policy (AUP) 486
  - Security-Related Human Resource Policy 487
  - Password Management and Complexity Policy 487
  - Personally Identifiable Information (PII) Policy 488
  - Disposal and Destruction Policy 489
  - Service Level Agreement (SLA) Policy 489
  - Classification of Information Policy 490
  - Change Management Policy 490
  - Ethics Policy 491

Education and Training 492
  - Organizational Training 492
  - Reducing Risks of Social Engineering 494

Chapter Summary 498
  - Key Terms 499
  - Review Questions 500
  - Hands-on Projects 503
  - Case Projects 507

APPENDIX A
## CompTIA Security+ 2008 Examination Objectives 509

APPENDIX B
## Security Web Sites 517
  - Security Organizations 517
  - Vendor Security Web Sites 518
Table of Contents

Threat Analysis 518
Standards Organizations and Regulatory Agencies 519
Laws Protecting Private Information 519
Blogs 520

APPENDIX C
Selected TCP/IP Ports and Their Threats 523

APPENDIX D
Sample Internet and E-Mail Acceptable Use Policy 527
College Z Department of Computer Information Systems Internet and E-Mail Acceptable Use Policy 527
Organizations ABC Acceptable Use Policy 530
1.0 Overview 530
2.0 Purpose 530
3.0 Scope 530
4.0 Policy 530
5.0 Enforcement 532
6.0 Definitions 532
7.0 Revision History 532

INDEX 533
Introduction

Security continues to be the number one concern of computer professionals today, and with good reason. Consider the evidence: as many as 150 million computers worldwide may be remotely controlled by attackers. Over 94 million credit and debit cards were compromised in one data security breach with losses totaling over $140 million. On average, every 39 seconds your computer is probed by attackers looking for vulnerabilities. One out of every 25 e-mails contains a virus. An organization on average receives 13.6 attacks each day. There are almost 8 million computer viruses on the loose. The median dollar loss for victims of ID theft is over $31,000. The number of US federal agencies that recently received a grade “F” on security is now eight. Over 15,000 freshly infected Web pages appear every day, and an unsuspecting user who only views one of these infected sites through their Web browser and does not even click on a link will find their computer infected. And over 1,500 users still respond to the “Nigerian General” spam each week.

As attacks continue to escalate, the need for trained security personnel also increases. Worldwide, the number of information security professionals will grow from 1.6 million in 2007 to 2.7 million in 2012, experiencing a compound annual growth rate of 10 percent. And unlike some information technology computer positions, security is not being offshored and is rarely outsourced.

Yet security personnel cannot be part of an “on-the-job training” program where an individual learns as they go; the risk is simply too great. Instead, many employers are requiring employees and job applicants to demonstrate their security knowledge and skills by possessing a security certification, such as the CompTIA Security+ certification. The Department of Defense Directive 8570 requires 110,000 information assurance professionals in assigned duty positions to have security certification within five years, and it also requires certification of all 400,000 full- and part-time military service members, contractors, and local nationals who are performing information assurance functions to be certified in security. And IT employers are willing to pay a premium for certified security personnel. Security certifications earn employees 10 percent to 14 percent more pay than their uncertified counterparts.

It is critical that computer users of all types understand how to protect themselves and their organizations from attacks. It is also important that individuals who want a job in the ever-growing field of information security be certified. Security+ Guide to Network Security Fundamentals, Third Edition is designed to meet both of these needs. This book takes a comprehensive view of the types of attacks that are launched against networks and computer systems. It examines computer security defense mechanisms, and offers practical tools, tips, and techniques to counter attackers. Security+ Guide to Network Security Fundamentals, Third Edition helps you defend against attackers and protect the most precious resource of all computer users and organizations—information. In addition, this book is a valuable tool for those who want to enter the field of information security. It provides you with the knowledge and skills that will help you prepare for the CompTIA Security+ certification exam.

Intended Audience

This book is intended to meet the needs of students and professionals who want to master practical network and computer security. A basic knowledge of computers and networks is all that is required to use this book. Those seeking to pass the Computing Technology Industry Association (CompTIA) Security+ certification exam will find the text’s approach and content especially helpful, because all Security+ 2008 exam objectives are covered. (For more

The book’s pedagogical features are designed to provide a truly interactive learning experience to help prepare you for the challenges of network and computer security. In addition to the information presented in the text, each chapter includes Hands-On Projects that guide you through implementing practical hardware, software, network, and Internet security configurations step by step. Each chapter also contains a running case study that places you in the role of problem solver, requiring you to apply concepts presented in the chapter to achieve a successful solution.

Chapter Descriptions
Here is a summary of the topics covered in each chapter of this book:

Chapter 1, “Introduction to Security,” begins by explaining the challenge of information security and why it is important. This chapter also introduces information security terminology and defines who are the attackers. In addition, it explains the CompTIA Security+ exam, and explores career options for those interested in mastering security skills.

Chapter 2, “System Threats and Risks,” examines the threats and risks that a computer system faces by looking at both software-based attacks and attacks directed against the computer hardware. It also examines the expanding world of virtualization and how virtualized environments are increasingly becoming the target of attackers.

Chapter 3, “Protecting Systems,” examines the steps for protecting systems by looking at steps that should be taken to harden the operating system, Web browser, Web servers, and how to protect from communications-based attacks. It also explores the additional security software applications that should be applied to systems.

Chapter 4, “Network Vulnerabilities and Attacks,” gives an overview of network security by examining some of the major weaknesses that are found in network systems. It also looks at the different categories of attacks and the methods of attacks that are commonly unleashed against networks today.

Chapter 5, “Network Defenses,” examines how to create a secure network through both network design and technologies and also how to apply network security tools to resist attacker.

Chapters 6, “Wireless Network Security,” explores security in a wireless network environment. It investigates the basic IEEE 802.11 security protections, the vulnerabilities associated with these protections, and examines today’s enhanced WLAN security protections for personal users as well as for enterprises.

Chapter 7, “Access Control Fundamentals,” introduces the principles and practices of access control by examining access control terminology, the three standard control models, and best practices. It also covers logical access control methods and explores physical access control.

Chapter 8, “Authentication,” examines the definition of authentication and reviews how it fits into access control. It explores authentication credentials and models, different types of authentication servers and authentication protocols, and remote authentication and security.
Chapter 9, “Performing Vulnerability Assessments” begins a study of performing vulnerability assessments. It defines risk and risk management and examines the components of risk management, and looks at ways to identify vulnerabilities so that adequate protections can be made to guard assets.

Chapter 10, “Conducting Security Audits,” explores users’ auditing privileges, auditing how subjects use those privileges, and monitoring tools and methods.

Chapter 11, “Basic Cryptography,” explores how encryption can be used to protect data. It covers what cryptography is and how it can be used for protection, how to protect data using three common types of encryption algorithms, and how to use cryptography on file systems and disks to keep data secure.

Chapter 12, “Applying Cryptography,” looks at practical methods for applying cryptography to protect data. The chapter explores digital certificates and how they can be used, public key infrastructure and key management, and how to use cryptography on data that is being transported.

Chapter 13, “Business Continuity,” covers the critical importance of keeping business processes and communications operating normally in the face of threats and disruptions. It explores how to prevent disruptions through protecting resources with environmental controls, and then looks at redundancy planning and disaster recovery procedures. Finally, the chapter studies how incident response procedures are used when an unauthorized event such as a security breach occurs.

Chapter 14, “Security Policies and Training,” looks at how organizations can establish and maintain security. It begins with a study of security policies and the different types of policies that are used, and then explores how education and training can help provide the tools to users to maintain a secure environment within the organization.

Appendix A, “CompTIA Security+ Examination Objectives,” provides a complete listing of the CompTIA Security+ 2008 certification exam objectives and shows the chapters in the book that cover material associated with each objective.

Appendix B, “Security Web Sites,” offers a listing of several important Web sites that contain security-related information.


Appendix D, “Sample Acceptable Use Policy,” gives a comprehensive example of two acceptable use policies.

Features
To aid you in fully understanding computer and network security, this book includes many features designed to enhance your learning experience.

• Maps to CompTIA Objectives. The material in this text covers all of the CompTIA Security+ 2008 exam objectives. In addition, the sequence of material follows closely the six Security+ domains.

• Chapter Objectives. Each chapter begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with both a quick reference to the chapter’s contents and a useful study aid.
Today’s Attacks and Defenses. Each chapter opens with a vignette of an actual security attack or defense mechanism that helps to introduce the material covered in that chapter.

Illustrations and Tables. Numerous illustrations of security vulnerabilities, attacks, and defenses help you visualize security elements, theories, and concepts. In addition, the many tables provide details and comparisons of practical and theoretical information.

Chapter Summaries. Each chapter’s text is followed by a summary of the concepts introduced in that chapter. These summaries provide a helpful way to review the ideas covered in each chapter.

Key Terms. All of the terms in each chapter that were introduced with bold text are gathered in a Key Terms list with definitions at the end of the chapter, providing additional review and highlighting key concepts.

Review Questions. The end-of-chapter assessment begins with a set of review questions that reinforce the ideas introduced in each chapter. These questions help you evaluate and apply the material you have learned. Answering these questions will ensure that you have mastered the important concepts and provide valuable practice for taking CompTIA’s Security+ exam.

Hands-On Projects. Although it is important to understand the theory behind network security, nothing can improve upon real-world experience. To this end, each chapter provides several Hands-On Projects aimed at providing you with practical security software and hardware implementation experience. These projects cover Windows Vista and Windows Server 2008 operating systems, as well as software downloaded from the Internet.

Case Projects. Located at the end of each chapter are several Case Projects. In these extensive exercises, you implement the skills and knowledge gained in the chapter through real design and implementation scenarios.

Text and Graphic Conventions
Wherever appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The icons used in this textbook are described below:

The Note icon draws your attention to additional helpful material related to the subject being described.

Tips based on the authors’ experience provide extra information about how to attack a problem or what to do in real-world situations.

The Caution icons warn you about potential mistakes or problems, and explain how to avoid them.
Each Hands-on activity in this book is preceded by the Hands-on icon and a description of the exercise that follows.

Case Project icons mark Case Projects, which are scenario-based assignments. In these extensive case examples, you are asked to implement independently what you have learned.

Test Preparation Software CD-ROM


Information Security Community Site

New to this edition is the Information Security Community Site. This site was created for students and instructors to find out about the latest in information security news and technology. Visit www.community.cengage.com/infosec to:

- Learn what’s new in information security through live news feeds, videos and podcasts.
- Connect with your peers and security experts through blogs and Ask the Author forums.
- Download student and instructor resources, such as additional labs, instructional videos, and instructor materials.
- Browse our online catalog.

Instructor’s Materials

The following additional 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 (ISBN: 1428340718). You can also retrieve these supplemental materials from the Course Technology Web site, www.course.com, by going to the page for this book, under “Download Instructor Files & Teaching Tools”.

Electronic Instructor’s Manual. The Instructor’s Manual that accompanies this textbook includes the following items: additional instructional material to assist in class preparation, including suggestions for lecture topics, tips on setting up a lab for the Hands-On Projects, and solutions to all end-of-chapter materials.

ExamView Test Bank. This Windows-based testing software helps instructors design and administer tests and pre-tests. In addition to generating tests that can be printed and administered, this full-featured program has an online testing component that allows students to take tests at the computer and have their exams automatically graded.

PowerPoint Presentations. This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom
presentations, to be made available to students on the network for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides for other topics introduced.

**Figure Files.** All of the figures and tables in the book are reproduced on the Instructor Resources CD. Similar to 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.

**Total Solutions for Security**


- This Lab Manual uses virtualized operating systems to teach students in a secure environment about attack and defense tools, different aspects of security applications, and how operating systems become vulnerable to attackers.

**LabSim for Security+** (ISBN: 1428340688)

- Lab simulations, demonstrations, video presentations and test preparation reinforce hands-on security skills. LabSim allows you to simulate hardware and operating systems on your computer without the need of additional hardware or software.

**Security+ Web-Based Labs** (ISBN: 142837695X)

- Using a real lab environment over the Internet, students can log on anywhere, anytime via a Web browser to gain essential hands-on experience in security using labs from *Security+ Guide to Network Security Fundamentals, 3e.*

**Security+ CourseNotes** (ISBN: 1435401255)

- Laminated quick reference card with vital information for CompTIA's Security+ exam, useful as a study aid, supplement to the textbook, or as a quick reference.

**WebCT/BB**

- Web CT and Blackboard are the leading distance learning solutions available today. Course Technology provides online content that fits into both platforms and includes the following components:
  - Topic reviews
  - Lecture notes
  - Case projects
  - Test banks
  - Practice exams
  - Custom syllabus, and more
What’s New with CompTIA Security+ Certification

The CompTIA Security+ exam was updated in October 2008 and is based on new Security+ exam objectives. There are several significant changes to the exam objectives. The number of exam objectives has been increased from five to six domains: Systems Security, Network Infrastructure, Access Control, Assessments and Audits, Cryptography, and Organizational Security. The new domain, Assessments and Audits, was added to address the importance of risk assessment and mitigation, as well as to cover the tools and techniques in addressing risk. In addition, each of the other domains has been reorganized and expanded to more accurately reflect current security issues and knowledge requirements. Finally, the exam objectives now place more importance on knowing “how to” rather than just knowing or recognizing security concepts. Here are the domains covered on the new Security+ exam:

<table>
<thead>
<tr>
<th>Domain</th>
<th>CompTIA Security+</th>
<th>Chapters in This Book</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Systems Security</td>
<td>21%</td>
<td>2, 3</td>
</tr>
<tr>
<td>2.0 Network Infrastructure</td>
<td>20%</td>
<td>4, 5, 6</td>
</tr>
<tr>
<td>3.0 Access Control</td>
<td>17%</td>
<td>7, 8</td>
</tr>
<tr>
<td>4.0 Assessments &amp; Audits</td>
<td>15%</td>
<td>9, 10</td>
</tr>
<tr>
<td>5.0 Cryptography</td>
<td>15%</td>
<td>11, 12</td>
</tr>
<tr>
<td>6.0 Organizational Security</td>
<td>12%</td>
<td>13, 14</td>
</tr>
</tbody>
</table>

How to Become CompTIA Certified

In order to become CompTIA certified, you must:

1. Select a testing center and a certification exam provider. For more information, visit the following Web site: http://certification.comptia.org/resources/registration.aspx

2. Register for and schedule a time to take the CompTIA certification exam at a convenient location.

3. Take and pass the CompTIA certification exam.

For more information about CompTIA’s certifications, please visit http://certification.comptia.org. CompTIA is a non-profit information technology (IT) trade association.

To contact CompTIA with any questions or comments, call (630) 678-8300 or send an e-mail to http://certification.comptia.org/customer_service/contact.aspx. The Computing Technology Industry Association (CompTIA) is the voice of the world’s information technology (IT) industry. Its members are the companies at the forefront of innovation; and the professionals responsible for maximizing the benefits organizations receive from their investments in technology.

CompTIA is dedicated to advancing industry growth through its educational programs, market research, networking events, professional certifications, and public policy advocacy. CompTIA is a not-for-profit trade information technology (IT) trade association. CompTIA’s certifications are designed by subject matter experts from across the IT industry. Each CompTIA certification is vendor-neutral, covers multiple technologies and requires demonstration of skills and knowledge widely sought after by the IT industry.
Acknowledgments

Although only the author’s name appears on the front cover of a book, it takes an entire team of dedicated professionals to create the finished product. And the team that produced this book was one of the very best. Executive Editor Stephen Helba once again showed his excellent vision by formulating the scope and direction of this book. It is a true privilege to be associated with Steve and his team. Senior Product Manager Michelle Cannistracri was very supportive and helped keep this project moving forward. Technical Editor Nicole Ashton carefully reviewed the book and identified many corrections. The team of peer reviewers evaluated each chapter and provided very helpful suggestions and contributions. Thanks to Scott Dawson, Spokane Community College, Dean Farwood, Heald College, Kim Fish, Butler County Community College, and David Pope, Ozarks Technical College.

Special recognition goes to Developmental Editor Deb Kaufmann. Not enough can be said about Deb. She was again superb at making suggestions, finding errors, taking care of all the small details, and somehow turning my rough work into polished prose. Deb is a joy to work with. Without question, Deb is simply the very best there is.

The entire Cengage/Course Technology staff was always very helpful and worked very hard to create this finished product. I’m honored to be part of such an outstanding group of professionals, and to these people and everyone on the team I extend my sincere thanks.

And finally, I want to thank my wonderful wife, Susan. Once again she provided patience, support, and love to see me through yet another book project. I simply could not have done any of it without her as my companion.

Dedication

To my wife, Susan, my sons and daughters-in-law Brian, Amanda, Greg and Megan, and my new grandson Braden.

About the Author

Mark Ciampa is Assistant Professor of Computer Information Systems at Western Kentucky University in Bowling Green, Kentucky, and holds a PhD from Indiana State University in Digital Communications. Prior to this he was Associate Professor and served as the Director of Academic Computing at Volunteer State Community College in Gallatin, Tennessee, for 20 years. Mark has worked in the IT industry as a computer consultant for the U.S. Postal Service, the Tennessee Municipal Technical Advisory Service, and the University of Tennessee. He is also the author of many Cengage/Course Technology textbooks, including CWNA Guide to Wireless LANs 2ed, Guide to Wireless Communications, Security+ Guide to Network Security Fundamentals 2ed, Security Awareness: Applying Practical Security In Your World, and Networking BASICS.
Lab Requirements

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. Appendix A pinpoints the exact chapter in which a specific Security+ exam objective is located.

Hardware and Software Requirements
Following are the hardware and software requirements needed to perform the end-of-chapter Hands-on Projects.

- Microsoft Windows Vista
- Windows 2008 Server
- An Internet connection and Web browser
- Microsoft Office 2007 or Office 2003
- Microsoft Office Outlook

Specialized Requirements
Whenever possible, the needs for specialized requirements were kept to a minimum. The following chapter features specialized hardware:


Free Downloadable Software Is Required in the Following Chapters:

Chapter 1:
- Secunia Software Inspector
- Microsoft Windows Malicious Software Removal Tool

Chapter 2:
- Microsoft RootkitRevealer
- SoftDD Keyboard Collector
- Irongeek Thumbscrew
- Microsoft Virtual PC 2007
- VMware Workstation

Chapter 3:
- GRC Securable
- EICAR AntiVirus Test File
- Microsoft Windows Vista Security Templates
- Microsoft Baseline Security Analyzer
Introduction

Chapter 4:
• Wireshark
• NetStumbler

Chapter 6:
• KLC Consulting SMAC

Chapter 7:
• Ophcrack
• KeePass

Chapter 9:
• Nessus
• GFI LANguard

Chapter 10:
• ThreatFire

Chapter 11:
• MD5DEEP
• TrueCrypt

Chapter 12:
• Comodo E-mail Certificate

Chapter 13:
• Briggs Software Directory Snoop

Chapter 14:
• Heidi Eraser
Security Certification: Market Drivers in Today’s Information Security Landscape

Contributed by Carol Balkcom, CompTIA Security+ Product Manager

We are seeing a rise in security training and certification today like never before. With companies incurring millions of dollars of potential liability in well-publicized security breaches, organizations—especially in the financial and healthcare industries, and government—have realized that they can no longer afford to have IT staff who are not proven and tested in the latest information security technologies and practices.

Today we also see the impact of U.S. military requirements on certification: Both military information assurance personnel and IT employees of government contractor companies who have contracts with the military are required to be certified, under the terms of their contracts. Included are many types of companies, from software, to systems integrators, to manufacture and service companies. This has implications for those who work for these companies, as well as those who would like to seek employment with them. There are government agencies such as the U.S. State Department that have special programs in place for their IT departments that require certification for new hires, as well as continuing education requirements for existing employees who want to be eligible for regular pay raises.

Evidence of the Need

Surveys show that criminal theft of information (with potentially disastrous consequences) can be traced in many cases to human error, failure to have adequate security policies, or failure to enforce existing policies. CompTIA security research published in 2008 showed that 30% of the most severe security breaches were caused by human error. Almost 60% of companies now require security training for IT staff, and roughly one-third of them now require certification. Eighty-nine percent of CompTIA survey respondents said that security certification had improved IT security. Without regular training and validation of knowledge, it is much more likely that employees in IT departments will lack the awareness or the motivation to use the rigorous methods required to secure their networks and mobile devices against intrusion.

“Vendor-Neutral” vs. “Vendor-Specific” Certification

When an IT professional decides to complement his or her experience with certification, a vendor-neutral certification is often the first type of exam taken. A vendor-neutral exam is one that tests for knowledge of a subject across platforms and products—without being tied to any specific product—while validating baseline skills and knowledge in that subject area. CompTIA exams are vendor-neutral exams and serve that portion of the IT population who have a good foundation in their chosen field and want to become certified. Individuals who take CompTIA Security+ are serious about their role in information security. They typically have at least two years of hands-on technical security experience. They may have also taken an exam like CompTIA Network+ as a first entry into certification.

1 Trends in Information Security: A CompTIA Analysis of IT Security and the Workforce, April 2008
Who Is Becoming Certified

There is a very long list of employers where significant numbers of staff in IT roles are becoming CompTIA Security+ certified. Here are some of the significant ones:


While the majority of CompTIA Security+ certified professionals are in North America, there are growing numbers in over 100 countries, with a solid and growing base especially in Japan, the UK, Germany, South Africa and South Korea. The need for information security training and certification has never been greater, and has become a worldwide issue.