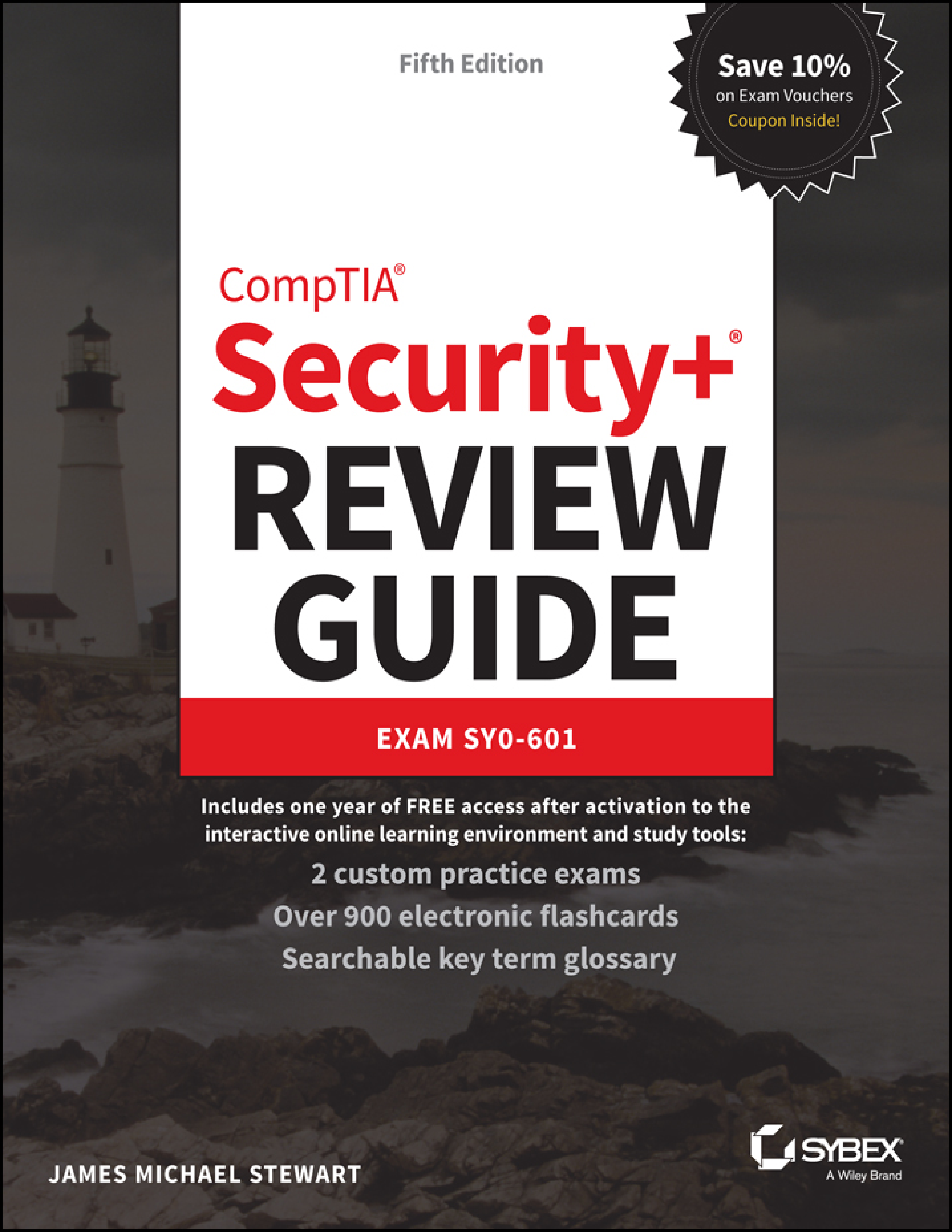

Fifth Edition

CompTIA® Security+® REVIEW GUIDE

EXAM SY0-601

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

2 custom practice exams
Over 900 electronic flashcards
Searchable key term glossary

JAMES MICHAEL STEWART

SYBEX
A Wiley Brand

Table of Contents

List of Tables

Chapter 1

Chapter 2

Chapter 3

List of Illustrations

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

CompTIA®
Security+® Review Guide

Exam SY0-601

Fifth Edition

James Michael Stewart

SYBEX®
A Wiley Brand

Published simultaneously in Canada

ISBN: 978-1-119-73538-0
ISBN: 978-1-119-73542-7 (ebk)
ISBN: 978-1-119-73536-6 (ebk)

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2020950195

To Catharine Renee Stewart:
You are my all and my everything, I love you.

Acknowledgments

Thanks to all those at Sybex/Wiley who continue to allow me to do what I enjoy most—impart knowledge to others. Thanks to Kenyon Brown, acquisitions editor, and the whole Sybex crew for professional juggling services supremely rendered. Thanks to my project editor, Kelly Talbot, my technical editor, Buzz Murphy, and my managing editor, Christine O'Connor. To my wonder woman of a wife, Cathy, and my amazing kids, Slayde and Remi—you make life exciting and sweet! To my mom, Johnnie: thanks for your love and consistent support. To Mark: go away or I shall taunt you a second time! Finally, as always, to Elvis: is the plural of Elvis … Elvises or Elvi?

—James Michael Stewart

About the Author

James Michael Stewart has been working with computers and technology since 1983 (although officially as a career since 1994). His work focuses on Internet technologies, professional certifications, and IT security. For over 20 years, Michael has been teaching job skill and certification focused courses, such as CISSP, CEH, CHFI, and Security+. Michael has contributed to many Security+ focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security and IT certification and administration topics, including being an author on the CISSP Study Guide 9th Edition. He has developed certification courseware and training materials and presented these materials in the classroom. He holds numerous certifications, including CEH, CHFI, ECSA, ECIH, CND, CySA+, PenTest+, CASP+, Security+, Network+, A+, CISSP, CISM, and CFR.

Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants, hands-on, “street smarts” experience. You can reach Michael by email at michael@impactonline.com.

About the Technical Editor

George (Buzz) Murphy, CISSP, CCSP, SSCP, CASP, is a public speaker, corporate trainer, author, and cybersecurity evangelist. A former Dell technology training executive and U.S. Army IT networking security instructor, he has addressed audiences at national conferences, international corporations and major universities. He has trained network and cybersecurity operators for the U.S. military branches, U.S. government security agencies, the Federal Reserve Bank, Sandia National Laboratory, Jet Propulsion Laboratory, Oak Ridge National Laboratory, and NASA.

As a military datacenter manager in Europe, Buzz has held top-secret security clearances in both US and NATO intelligence and through the years has earned more than 30 IT and cybersecurity certifications from CompTIA, (ISC)^2, PMI, Microsoft, and other industry certification organizations.

Buzz has authored or been the technical editor on numerous books on a wide range of topics including network engineering, industrial control technology, IT security, and more, including various editions of *CASP: CompTIA Advanced Security Practitioner Study Guide*, *CompTIA Security+ Study Guide*, *SSCP: Systems Security Practitioner Study Guide*, and *CCFP: Certified Cyber Forensics Professional Certification Guide*.

Introduction

The Security+ certification program was developed by the Computer Technology Industry Association (CompTIA) to provide an industry-wide means of certifying the competency of computer service technicians in the basics of computer security. The Security+ certification is granted to those who have attained the level of knowledge and security skills that show a basic competency in the security needs of both personal and corporate computing environments. CompTIA's exam objectives are periodically updated to keep their exams applicable to the most recent developments. The most recent update, labeled SY0–601, occurred in late 2020.

What Is Security+ Certification?

The Security+ certification was created to offer an introductory step into the complex world of IT security. You need to pass only a single exam to become Security+ certified. However, obtaining this certification doesn't mean you can provide realistic security services to a company. In fact, this is just the first step toward developing and demonstrating real-world security knowledge and experience. By obtaining Security+ certification, you should be able to acquire more security experience in order to pursue more complex and in-depth security knowledge and certification.

If you have further questions about the scope of the exams or related CompTIA programs, as well as to confirm the latest pricing for the exam, refer to the CompTIA website at `www.comptia.org`. For details on the exam registration procedures, please visit `www.vue.com`.

Is This Book for You?

CompTIA® Security+® Review Guide: Exam SY0-601 is designed to be a succinct, portable exam reference book and review guide. It can be used in conjunction with a more typical study guide, such as Wiley's *CompTIA Security+ Study Guide: SY0-601*, with a practice questions resource, such as Wiley's *CompTIA Security+ Practice Tests: Exam SY0-601*, with computer-based training (CBT) courseware and a classroom/lab environment, or as an exam review for those who don't feel the need for more extensive (and/or expensive) test preparation. It is my goal to identify those topics on which you can expect to be tested and to provide sufficient coverage of these topics.

Perhaps you've been working with information technologies for years. The thought of paying lots of money for a specialized IT exam-preparation course probably doesn't sound appealing. What can they teach you that you don't already know, right? Be careful, though—many experienced network administrators have walked confidently into the test center only to walk sheepishly out of it after failing an IT exam. After you've finished reading this book, you should have a clear idea of how your understanding of the technologies involved matches up with the expectations of the Security+ test crafters. My goal is to help you understand new technologies that you might not have thoroughly implemented or experienced yet as well as give you a perspective on solutions that might lie outside of your current career path.

Or perhaps you're relatively new to the world of IT, drawn to it by the promise of challenging work and higher salaries. You've just waded through an 800-page study guide or taken a weeklong class at a local training center. Lots of information to keep track of, isn't there? Well, by organizing this book according to CompTIA's exam objectives, and by breaking up the information into concise, manageable pieces, I have created what I think is the handiest exam review guide available. Throw it in your backpack or obtain the digital version and carry it around with you. As you read through this book, you'll be able to quickly identify those areas in which you have confident knowledge and those that require a more in-depth review.

How Is This Book Organized?

This book is organized according to the official objectives list prepared by CompTIA for the Security+ exam. The chapters correspond to the five major domains of objective and topic groupings. The exam is weighted across these five topical areas or domains as follows:

- 1.0 Threats, Attacks, and Vulnerabilities (24%)
- 2.0 Architecture and Design (21%)
- 3.0 Implementation (25%)
- 4.0 Operations and Incident Response (16%)
- 5.0 Governance, Risk, and Compliance (14%)

> NOTE
>
> The previous SY0-501 version of Security+ was organized around six domains.

Within each chapter, all of the exam objectives from each domain are addressed in turn and in order according to the official exam objectives directly from CompTIA. In addition to a discussion of each objective, every chapter includes two additional specific features: Exam Essentials and Review Questions.

Exam Essentials At the end of each subdomain objective section, you're given a list of topics that you should explore fully before taking the test. Included in the “Exam Essentials” sections are notations of the key information you should have absorbed from that section. These items represent the minimal knowledge you should retain from each chapter section.

> **Review Questions** This feature ends every chapter and provides 20 questions to help you gauge your mastery of the chapter. For each question you get wrong, take the time to research why the right answer is correct and why your wrong answer was incorrect. This helps you learn what you don't know so you can more effectively handle similar questions in the future.

This book was not designed to be read cover to cover, but you are welcome to do so. The organization is based directly on that provided by CompTIA in its official Certification Exam Objective's list. This organization is not necessarily always ideal for the order of topics or the grouping of topics. However, this organization was chosen to make it as easy as possible to locate material related to specific objective items. If you need to read about a specific topic and know where it is on the objective list, then you can quickly locate it in the pages of this book. First locate the chapter, then the relevant top-level heading, and then the specific heading whether it is one, two, or three heading levels below that.

If a topic is included more than once in the objectives, it is usually covered once (and usually at its first occurrence), and then this location is referenced under the other heading locations where it appears again.

As you go over the material in the book, you are also going to discover that CompTIA did not include all relevant concepts or keywords for a particular topic. When needed, we added or expanded coverage within the objective headings to include foundational, background, or relevant material. There are even a few occurrences where a topic was divided into multiple objectives and then those objects spread across multiple sections. These are treated like repeats, where full coverage is included in the first instance of the first topic and references back to this coverage are placed under the other related headings. For example, “card cloning” and “skimming” are the same thing, so it is covered under “card cloning,” and a reference to that coverage is listed under “skimming.”

Interactive Online Learning Environment and Test Bank

We've included several additional test-preparation features on the interactive online learning environment. These tools will help you retain vital exam content as well as prepare you to sit for the actual exams.

> Go to `www.wiley.com/go/sybextestprep` to register and gain access to this interactive online learning environment and test bank with study tools.

Sample Tests In this section, you'll find the chapter tests, which present all the review questions from the end of each chapter, as well as two more unique practice tests of 90 questions each. Use these questions to test your knowledge of the study guide material.

Electronic Flashcards Questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

Glossary of Terms in PDF We have included a very useful glossary of terms in PDF format so you can easily read it on any computer. If you have to travel and brush up on any key terms, you can do so with this useful resource.

Tips for Taking the Security+ Exam

Most CompTIA exams can be taken in-person at a Pearson Vue testing facility or via an online exam portal. You can elect which test delivery method you want to use when you register for your exam at `vue.com`.

Here are some general tips for taking your exam successfully:

- Bring two forms of ID with you. One must be a photo ID, such as a driver's license. The other can be a major credit card or a passport. Both forms must include a signature.
- Arrive early at the exam center so you can relax and review your study materials. Be connected early if you are taking an online exam. Being 15 minutes early is usually plenty.
- Read the questions carefully. Don't be tempted to jump to an early conclusion. Make sure you know exactly what the question is asking.
- Read each question twice, read the answer options, and then read the question again before selecting an answer.
- You can move forward and backward through the exam, but only one question at a time. Only after reaching the Review Page after the last question can you jump around among the questions at random.
- Don't leave any unanswered questions. Unanswered questions give you no opportunity for guessing correctly and scoring more points.

- Watch your clock. If you have not seen your last question when you have five minutes left, guess at the remaining questions.
- There will be questions with multiple correct responses. When there is more than one correct answer, a message on the screen will prompt you to either “Choose two” or “Choose all that apply.” Be sure to read the messages displayed so you know how many correct answers you must choose.
- Questions needing only a single correct answer will use radio buttons to select an answer, whereas those needing two or more answers will use check boxes.
- When answering multiple-choice questions you're not sure about, use a process of elimination to get rid of the obviously incorrect answers first. Doing so will improve your odds if you need to make an educated guess.
- Try to expand your perspective from your own direct experience. Often the writers of the exam questions are from large enterprises; if you only consider answers in light of a small company, military branch, or as an individual, you might not determine the correct answer.
- You can mark or flag a question to indicate you want to review it again before ending the exam. Flagged questions will be highlighted on the Review page. However, you must complete your review before your exam time expires.
- Many exam questions will combine concepts and terms from multiple topics/domains to make the question more challenging. Attempt to figure out the core concept being focused on. Often, the answer options will provide guidance as to the focus of the question, especially if the question text itself is not direct and obvious enough.

- For the latest pricing on the exams and updates to the registration procedures, visit CompTIA's website at www.comptia.org.

Performance-Based Questions

CompTIA has begun to include performance-based (scenario-based) questions on its exams. These differ from the traditional multiple-choice questions in that the candidate is expected to perform a task or series of tasks. Tasks could include filling in a blank, answering questions based on a video or an image, reorganizing a set into an order, placing labels on a diagram, filling in fields based on a given situation or set of conditions, or setting the configuration on a network security management device. Don't be surprised if you are presented with a scenario and asked to complete a task. The performance-based questions are designed to be more challenging than standard multiple-choice questions and thus are also worth more points. Take the time to answer these carefully. For an official description of performance-based questions from CompTIA, visit www.comptia.org/blog/what-is-a-performance-based-question- (Note: the final dash is needed; you can also search to find this page with the phrase “What Is A Performance-Based Question?”) and www.comptia.org/testing/testing-options/about-comptia-performance-exams/performance-based-questions-explained (this second link is from the CompTIA Security+ information page, so you can follow it from there instead of typing it in).

Exam Specifics

The Security+ SY0-601 exam consists of up to 90 questions with a time allotment of 90 minutes for the exam itself. Additional time is provided for the pre-exam elements, such as the NDA, copyright disclosures, and the post-exam survey. If you were to be assigned only multiple-choice questions, then you would have the maximum of 90 questions. If you are assigned performance-based questions (which is most likely), then you will have fewer than 90 total questions. It is fairly common to have 5 or 6 performance-based questions and about 70 multiple-choice questions, for a total of 75 or so questions. However, you could be assigned 8 or more performance-based questions with about 50 multiple-choice questions, for a total of 55 questions. You will know exactly how many questions you have been assigned in total once the first question is displayed on the screen, by reading the “1 out of ##” line located in the top corner. You will discover how many performance-based questions you were assigned only by working through all of the questions and counting them as you encounter them. Usually most performance-based questions are located as the first of your questions, but CompTIA could position one or two elsewhere in your test bank.

To pass, you must score at least 750 points on a scale of 100–900 (effectively 81.25%). At the completion of your test, you will receive a printout of your test results. This report will show your score and the objective topics about which you missed a question. This printout will seem oddly long, even if you pass, as many multiple-choice questions cover four topics, so getting one question wrong could add four lines of topics to this list.

> NOTE
>
> Although there is no clear statement from CompTIA, there seem to be some questions on the exam that are included for evaluation purposes but do not count toward your score. These questions are likely on topics not currently listed in the SY0-601 objectives list, and they will appear at random within your exam and will not be marked in any way.

> NOTE
>
> These details are subject to change. For current information, please consult the CompTIA website: www.comptia.org.

The Security+ Exam Objectives

The exam objectives were used as the structure of this book. I use the objective list's order and organization throughout the book. Each domain is covered in one chapter. Each objective, subobjective (i.e., bulleted topic), and sub-subobjective (i.e., second-level bulleted topic) is a heading within a chapter.

In the text, I reference locations of topics by their section or objective number (such as section 2.3) and the heading of the content (such as “Quality Assurance (QA)”). The first number of an objective section is this book's chapter number, and the second number is the top-level heading within the chapter.