Introduction

The Security+ certification was developed by the Computer Technology Industry Association (CompTIA) to provide an industrywide means of certifying the competency of computer and network administrators in the basics of securing their systems and networks. The security professional's job is to protect the confidentiality, integrity, and availability of the organization's valuable information assets.

According to CompTIA, the Security+ certification

> "validates knowledge of communication security, infrastructure security, cryptography, operational security, and general security concepts. It is an international, vendor-neutral certification that is taught at colleges, universities and commercial training centers around the world. Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years on-the-job networking experience, with an emphasis on security. The CompTIA Network+ certification is also recommended. Because human error is the number one cause for a network security breach, CompTIA Security+ is recognized by the technology community as a valuable credential that proves competency with information security. Major corporations such as Sun, IBM/Tivoli Software Group, Symantec, Motorola, Hitachi Electronics Services, and VeriSign value the CompTIA Security+ certification and recommend or require it of their IT employees."

Although most books that target certification candidates present material for you to memorize before the exam, this book is different. It guides you through procedures and tasks that solidify related concepts, thus allowing you to devote your memorization efforts to more abstract theories because you've mastered the practical topics through doing. Even if you do not aspire to become a security professional, this book might still be a valuable primer for your career.

What Is Security+ Certification?

The Security+ certification was created to offer an introductory step into the complex world of PC and laptop hardware and software support.

Security+ candidates must take the Security+ exam (Exam #SY0-101), which covers various security concepts.

A detailed list of the Security+ SY0-101 exam objectives is presented in this introduction; see the section "The Security+ Exam Objectives."

Obtaining the Security+ certification does not mean you can provide sufficient system and network security services to a company. In fact, this is just the first step toward true technical knowledge and experience. By obtaining Security+ certification, you will be able to obtain more computer and network security administration experience in order to pursue more complex and in-depth knowledge and certifications.

For the latest pricing on the exam and updates to the registration procedures, call either Thomson Prometric at (866) 776-6387 or (800) 776-4276, or Pearson VUE at (877) 551-7587. You can also go to either `http://www.2test.com` or `http://www.prometric.com` (for Thomson Prometric) or `http://www.vue.com` (for Pearson VUE) for additional information or to register online. If you have further questions about the scope of the exams or related CompTIA programs, refer to the CompTIA website at `http://www.comptia.org`.

Is This Book for You?

Security Administrator Street Smarts is designed to give you insight into the world of a typical system and network security technician by walking you through some of the daily tasks you can expect on the job. We recommend that you invest in certain equipment to get the full effect from this book. However, much value can be derived from simply reading through the tasks without performing the steps on live equipment. Organized classes and study groups are the ideal structures for obtaining and practicing with the recommended equipment.

The *CompTIA Security+ Study Guide, Third Edition* (Sybex, 2006) is a recommended companion to this book in your studies for the CompTIA Security+ certification.

How This Book Is Organized

This book is organized into an initial system setup procedure, followed by 10 phases. Each phase is separated into individual tasks. The phases represent broad categories under which related responsibilities are grouped. The tasks within each phase lead you step by step through the processes required for successful completion. When performed in order, the tasks in this book approximate those required by a system security administrator over an extended period of time. The phases and their descriptions are as follows:

- *Administrative System Setup* walks you through the process of converting a system from a standard user's "warm and fuzzy" system into a highly refined administrative tool,

where you have complete vision of and access to the system components, as well as easy access to a collection of powerful administrative tools.

- *Phase 1—The Grunt Work of Security* presents the initial, and essential, objectives that a security professional needs to have in place to understand, establish the basis for, implement, and enforce security within an organization.
- *Phase 2—Hardening Systems* shows you where the most common vulnerabilities exist within a system; the attack points; how to identify them, and how to minimize the attack surface of a system.
- *Phase 3—Protecting Against Malware* shows you how to implement filters, scanners, and other tools to defend the system against inbound threats, such as viruses, worms, spyware, and rootkits.
- *Phase 4—Secure Storage* provides real-world tools and techniques to ensure that data, while residing on a system, will remain secure. Discussed are the use of encryption, the assignment of permissions following the principle of least privilege, and the implementation of fault tolerance.
- *Phase 5—Managing User Accounts* presents procedures related to its user accounts that every computer network should have implemented. These procedures include implementing a strong password policy and securing default user accounts, such as the Administrator and the Guest accounts.
- *Phase 6—Network Security* shows you how to configure encryption for data while it's in transit on the corporate network, and between the telecommuter and the corporate headquarters (via VPNs). Further, it shows how to configure basic firewall rules, and how to configure a wireless network with acceptable security using 802.11i and WPA.
- *Phase 7—Securing Internet Activity* shows you how to secure your Microsoft Internet Explorer, e-mail, and IP settings, and how to use digital certificates in a Public Key Infrastructure (PKI) environment.
- *Phase 8—Security Testing* presents the use of security assessment tools to evaluate the general strength of a system, and penetration-testing tools to view your systems as an attacker would see them.
- *Phase 9—Investigating Incidents* shows you how to operate like a forensics investigator, and how to track down and uncover hidden details of some earlier security-related event. You will learn how to configure auditing and review audit logs, how to perform a memory dump to record the contents of physical RAM, how to recover deleted files and folders, and how to use and understand a sniffer on the network to view the network traffic.
- *Phase 10—Security Troubleshooting* examines multiple procedures to perform disaster recovery and focuses on Safe mode, Last Known Good Configuration, and System Recovery. It also looks at procedures and tools to sanitize media for secure destruction of confidential data to allow for reuse of magnetic media.

Each task in this book is organized into sections aimed at giving you what you need when you need it. The first section introduces you to the task and any key concepts that can assist you in understanding the underlying technology and the overall procedure. The following describes the remaining sections:

- *Scenario*—This section places you in the shoes of the PC support technician, describing a situation in which you will likely find yourself. The scenario is closely related to and often solved by the task at hand.
- *Scope of Task*—This section is all about preparing for the task. It gives you an idea of how much time is required to complete the task, what setup procedure is needed before beginning, and any concerns or issues to look out for.
- *Procedure*—This is the actual meat of the task itself. This section lists the equipment required to perform the task in a lab environment. It also gives you the ordered steps to complete the task.
- *Criteria for Completion*—This final section briefly explains the outcome you should expect after completing the task. Any deviation from the result described is an excellent reason to perform the task again and watch for sources of the variation.

How to Contact the Publisher

Sybex welcomes feedback on all of its titles. Visit the Sybex website at `http://www.sybex.com` for book updates and additional certification information. You'll also find forms you can use to submit comments or suggestions regarding this or any other Sybex title.

How to Contact the Authors

David R. Miller and Michael Gregg welcome your questions and comments. You can reach them by e-mail at `DMiller@MicroLinkCorp.com` and `MikeG@thesolutionfirm.com`, respectively.

The Security+ Exam Objectives

The Security+ exams are made up of the mandatory Security+ exam. The following presents the detailed exam objectives of each test.