Third Edition

CompTIA® CASP+ STUDY GUIDE

EXAM CAS-003

Includes interactive online learning environment and study tools:

2 custom practice exams

100 electronic flashcards

Searchable key term glossary

JEFF T. PARKER AND MICHAEL GREGG

SYBEX®
A Wiley Brand

CompTIA®

CASP+®

Study Guide

Third Edition

CompTIA®

CASP+® Advanced Security Practitioner

Study Guide Exam CAS-003

Third Edition

Jeff T. Parker

Michael Gregg

SYBEX®
A Wiley Brand

Senior Acquisitions Editor: Kenyon Brown
Development Editor: Gary Schwartz
Technical Editors: Russ Christy and Brent Hamilton
Senior Production Editor: Christine O'Connor
Copy Editor: Judy Flynn
Editorial Manager: Pete Gaughan
Production Manager: Kathleen Wisor
Executive Editor: Jim Minatel
Book Designers: Judy Fung and Bill Gibson
Proofreader: Nancy Carrasco
Indexer: Johnna VanHoose Dinse
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley

Cover Image: Getty Images Inc./Jeremy Woodhouse

Published simultaneously in Canada

ISBN: 978-1-119-47764-8
ISBN: 978-1-119-47771-6 (ebk.)
ISBN: 978-1-119-47767-9 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2018967329

10 9 8 7 6 5 4 3 2 1

To my wife, Maylia:

Thank you for your encouragement, patience, and support.
CC&W, Jeff

Acknowledgments

Kudos to the Sybex/Wiley team, but particularly Pete Gaughan and Kenyon Brown for granting me the opportunity to bring this edition to the reader. Thank you as well to Gary Schwartz for his early support and patience to the end. Finally, much thanks to Russ Christy and Brent Hamilton for their vigilance as the technical editors.

About the Authors

Jeff Parker resides on the Canadian east coast, but he works for an IT consultancy firm in Virginia where he specializes in IT risk management and compliance. Jeff started in information security while working as a software engineer for HP in Boston, Massachusetts. Jeff then took the role of a global IT risk manager for Deutsche Post to enjoy Prague in the Czech Republic with his family for several years. There he developed and oversaw implementation of a new IT risk management strategy. Today, Jeff most enjoys time with his two children in Nova Scotia.

Jeff maintains several certifications, including CISSP, CompTIA CASP+, CySA+, and ITT+. He also co-authored the book *Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework* (Wiley, 2017) with Jessey Bullock. Jeff also wrote practice exam books for the CompTIA certifications CySA+ and the A+, out in 2018 and 2019, respectively.

Michael Gregg is the founder and CEO of Superior Solutions, Inc., a security consulting firm based in Houston, Texas. Superior Solutions performs security assessments and penetration testing for Fortune 1000 firms. The company has performed security assessments for private, public, and governmental agencies. Its Houston-based team travels the United States to assess, audit, and provide training services.

Michael is responsible for working with organizations to develop cost-effective and innovative technology solutions to security issues and for evaluating emerging technologies. He has more than 20 years of experience in the IT field and holds two associate's degrees, a bachelor's degree, and a master's degree. In addition to co-writing the first, second, and third editions of *Security Administrator Street Smarts*, Michael has written or co-written 14 other books, including *Build Your Own Security Lab: A Field Guide for Network Testing* (Wiley, 2008), *Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network* (Syngress, 2007), *Certified Ethical Hacker Exam Prep 2* (Pearson, 2006), and *Inside Network Security Assessment: Guarding Your IT Infrastructure* (Sams Publishing, 2005).

Michael has been featured on Fox News, CBS News, CNN, and other TV outlets as well as in the *New York Times* and other print publications, and he has testified before US Congress as an industry/cybersecurity expert. Michael has created over a dozen training security classes and training manuals and has created and performed video instruction on many security topics such as cybersecurity, CISSP, CISA, Security+, and others.

When not consulting, teaching, or writing, Michael enjoys 1960s muscle cars and giving back to the community. He is a member of the board of Habitat for Humanity.

Contents at a Glance

Contents

Table of Exercises

Introduction

The CASP+ certification was developed by the Computer Technology Industry Association (CompTIA) to provide an industry-wide means of certifying the competency of security professionals who have 10 years' experience in IT administration and at least 5 years' hands-on technical experience. The security professional's job is to protect the confidentiality, integrity, and availability of an organization's valuable information assets. As such, these individuals need to have the ability to apply critical thinking and judgment.

According to CompTIA, the CASP+ certification "is a vendor-neutral credential." CASP+ validates "advanced-level security skills and knowledge" internationally. There is no prerequisite, but "CASP+ certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, 'hands-on' focus at the enterprise level."

Many certification books present material for you to memorize before the exam, but this book goes a step further in that it offers best practices, tips, and hands-on exercises that help those in the field of security better protect critical assets, build defense in depth, and accurately assess risk.

If you're preparing to take the CASP+ exam, it is a good idea to find out as much information as possible about computer security practices and techniques. Because this test is designed for those with years of experience, you will be better prepared by having the most hands-on experience possible; this study guide was written with this in mind. We have included hands-on exercises, real-world scenarios, and review questions at the end of each chapter to give you some idea as to what the exam is like. You should be able to answer at least 90 percent of the test questions in this book correctly before attempting the exam; if you're unable to do so, reread the problematic chapters and try the questions again. Your score should improve.

Before You Begin the CompTIA CASP+ Certification Exam

Before you begin studying for the exam, it's good for you to know that the CASP+ exam is offered by CompTIA (an industry association responsible for many certifications) and is granted to those who obtain a passing score on a single exam. Before you begin studying for the exam, learn all you can about the certification.

A detailed list of the CASP+ CAS-003 (2018 Edition) exam objectives is presented in this Introduction. See the section "The CASP+ (2018 Edition) Exam Objective Map."

Obtaining CASP+ certification demonstrates that you can help your organization design and maintain system and network security services designed to secure the organization's assets. By obtaining CASP+ certification, you show that you have the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments.

Who Should Read This Book

The *CASP+ CompTIA Advanced Security Practitioner Study Guide: Exam CAS-003, 3rd Edition*, is designed to give you the insight into the working world of IT security, and it describes the types of tasks and activities that a security professional with 5–10 years of experience carries out. Organized classes and study groups are the ideal structures for obtaining and practicing with the recommended equipment.

College classes, training classes, and boot camps are recommended ways to gain proficiency with the tools and techniques discussed in the book. However, nothing delivers hands-on learning like experiencing your own attempts, successes, and mistakes—on a home lab. More on home labs later.

What You Will Learn

This *CASP+ CompTIA Advanced Security Practitioner Study Guide* covers all you need to know in order to pass the CASP+ exam. The exam is based on exam objectives, and this study guide is based on the current iteration of the CASP+ exam, version CAS-003.

The latest exam version was first released in April 2018 and, if the CASP+ exam version life cycle follows the same pattern as most CompTIA exams, the CAS-003 version will remain current for about three years.

Per the CASP+ CompTIA objectives for exam version CAS-003, the five domains include the following:

- Risk Management
- Enterprise Security Architecture
- Enterprise Security Operations
- Technical Integration of Enterprise Security
- Research, Development, and Collaboration