

Third Edition

Save 10%

on Exam Vouchers

Coupon Inside!

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

**Take the Next Step
in Your IT Career**

**Save
10%
on Exam Vouchers***
(up to a \$35 value)

CompTIA®

Get details at
sybex.com/go/comptiavoucher

*Some restrictions apply. See web page for details.



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
Copyright © 2019 by John Wiley & Sons, Inc., Indianapolis, Indiana

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

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

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 <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2018967329

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CompTIA and CASP are registered trademarks of CompTIA Properties, LLC. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

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 Jesse 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

<i>Introduction</i>		<i>xxvii</i>
<i>Assessment Test</i>		<i>lxi</i>
Chapter 1	Cryptographic Tools and Techniques	1
Chapter 2	Comprehensive Security Solutions	47
Chapter 3	Securing Virtualized, Distributed, and Shared Computing	97
Chapter 4	Host Security	143
Chapter 5	Application Security and Penetration Testing	195
Chapter 6	Risk Management	265
Chapter 7	Policies, Procedures, and Incident Response	313
Chapter 8	Security Research and Analysis	357
Chapter 9	Enterprise Security Integration	413
Chapter 10	Security Controls for Communication and Collaboration	459
Appendix A	Answers to Review Questions	519
Appendix B	CASP+ Lab Manual	533
<i>Index</i>		<i>591</i>

Contents

Introduction

xxvii

Assessment Test

lxi

Chapter 1	Cryptographic Tools and Techniques	1
	The History of Cryptography	3
	Cryptographic Services	4
	Cryptographic Goals	4
	Cryptographic Terms	6
	Cipher Types and Methods	9
	Symmetric Encryption	10
	Data Encryption Standard	12
	Triple DES	14
	Rijndael	14
	Advanced Encryption Standard	14
	International Data Encryption Algorithm	15
	Rivest Cipher Algorithms	15
	Asymmetric Encryption	16
	Diffie–Hellman	17
	RSA	18
	Elliptic Curve Cryptography	18
	ElGamal	18
	Hybrid Encryption	19
	Hashing	20
	Hashing and Message Digests	20
	Digital Signatures	23
	Public Key Infrastructure	25
	Certificate Authority	26
	Registration Authority	26
	Certificate Revocation List	27
	Digital Certificates	27
	Certificate Distribution	29
	The Client’s Role in PKI	31
	Implementation of Cryptographic Solutions	32
	Application Layer Encryption	33
	Transport Layer Encryption	34
	Internet Layer Controls	35
	Physical Layer Controls	36
	Cryptocurrency	37
	Blockchain	37
	Steganography	38

	Cryptographic Attacks	39
	Summary	40
	Exam Essentials	41
	Review Questions	43
Chapter 2	Comprehensive Security Solutions	47
	Advanced Network Design	50
	Network Authentication Methods	50
	Placement of Fixed/Mobile Devices	50
	Placement of Hardware and Application	51
	802.1x	51
	Mesh Networks	51
	Remote Access	52
	Virtual Networking and Placement of Security Components	54
	SCADA	58
	VoIP	59
	TCP/IP	61
	Network Interface Layer	62
	Internet Layer	64
	Transport Layer	70
	Application Layer	72
	Secure Communication Solutions	75
	Network Data Flow	75
	SSL Inspection	76
	Domain Name Service	76
	Securing Zone Transfers	77
	Start of Authority	78
	Secure DNS	79
	Transaction Signature	80
	Fast Flux DNS	80
	Lightweight Directory Access Protocol	81
	Secure Directory Services	81
	Active Directory	82
	Security Information and Event Management	82
	Database Activity Monitoring	82
	Federated ID	82
	Single Sign-On	83
	Kerberos	83
	Secure Facility Solutions	83
	Building Layouts	84
	Facilities Manager	85
	Secure Network Infrastructure Design	85
	Router Configuration	87
	Enterprise Service Bus	89
	Web Services Security	89

	Summary	90
	Exam Essentials	90
	Review Questions	93
Chapter 3	Securing Virtualized, Distributed, and Shared Computing	97
	Enterprise Security	100
	Software-Defined Networking	102
	Cloud Computing	104
	Cloud Service Models	104
	Cloud Computing Providers and Hosting Options	105
	Benefits of Cloud Computing	106
	Security of On-Demand/Elastic Cloud Computing	109
	Data Sovereignty	113
	Cloud Computing Vulnerabilities	114
	Cloud Storage	116
	Cloud-Augmented Security Services	117
	Virtualization	119
	Virtual Desktop Infrastructure	119
	Virtualized Servers	120
	Virtual LANs	126
	Virtual Networking and Security Components	127
	Enterprise Storage	129
	Summary	136
	Exam Essentials	136
	Review Questions	138
Chapter 4	Host Security	143
	Firewalls and Network Access Control	147
	Host-Based Firewalls	152
	Persistent Agent	155
	Non-Persistent Agent	155
	Agent-Based Technology	156
	Agentless-Based Technology	156
	Trusted Operating Systems	156
	Endpoint Security Solutions	160
	Common Threats to Endpoint Security	162
	Anti-Malware	164
	Antivirus	165
	Hunt Teaming	167
	Anti-Spyware	168
	Spam Filters	169
	Host Hardening	171
	Asset Management	176

	Data Exfiltration	177
	External I/O Restrictions on Hardware	179
	Intrusion Detection and Prevention	180
	Network Management, Monitoring, and Security Tools	185
	Security Devices	186
	Operational and Consumer Network-Enabled Devices	186
	Summary	188
	Exam Essentials	188
	Review Questions	190
Chapter 5	Application Security and Penetration Testing	195
	Application Security Design Considerations	201
	Specific Application Issues	204
	Cross-Site Scripting (XSS)	205
	Cross-Site Request Forgery	205
	Improper Error Handling	206
	Geotagging	206
	Clickjacking	207
	Session Management	207
	Input Validation	208
	SQL Injection	209
	Application Sandboxing	210
	Application Security Frameworks	211
	Software Assurance	212
	Standard Libraries	212
	NX/XN Bit Use	213
	ASLR Use	213
	Code Quality	214
	Code Analyzers	214
	Development Approaches	214
	DevOps	215
	Waterfall Approach	215
	Incremental Approach	215
	Spiral Approach	215
	Continuous Integration	216
	Versioning	216
	Secure Coding Standards	216
	Documentation	217
	Requirements Definition	218
	Security Requirements Traceability Matrix (SRTM)	218
	System Design Document	218
	Test Plans	218
	Validation and Acceptance Testing	219
	Regression	219
	User Acceptance Testing	219

Unit Testing	219
Integration Testing	219
Peer Review	220
Application Exploits	220
Privilege Escalation	221
Improper Storage of Sensitive Data	222
Secure Cookie Storage and Transmission	222
Context-Aware Management	224
Geolocation/Geofencing	224
User Behavior	224
Time-based Restrictions	225
Security Restrictions	225
Malware Sandboxing	225
Pivoting	226
Open-Source Intelligence	226
Social Media	227
WHOIS	227
Routing Tables	227
DNS Records	227
Memory Dumping	227
Client-Side Processing vs. Server-Side Processing	228
JSON/REST	229
Browser Extensions	229
Ajax	229
JavaScript/Applets	229
Flash	230
HTML5	231
SOAP	231
Web Services Security	231
Buffer Overflow	232
Memory Leaks	233
Integer Overflow	233
Race Conditions (TOC/TOU)	234
Resource Exhaustion	235
Data Remnants	235
Use of Third-Party Libraries	236
Code Reuse	236
Security Assessments and Penetration Testing	236
Test Methods	236
Penetration Testing Steps	237
Assessment Types	238
Red, Blue, and White Teaming	240
Red Team: The Bad Guys	240
Blue Team: The Good Guys	241
White Team: The Judge and Jury	241

Vulnerability Assessment Areas	241
Security Assessment and Penetration Test Tools	243
Footprinting Tools	244
Port Scanning Tools	246
Fingerprinting Tools	248
Vulnerability Scanners	249
Protocol Analyzer Tools	250
Passive Vulnerability Scanners	252
SCAP Scanners	253
Network Enumeration Tools	253
Visualization Tools	254
File Integrity Monitoring Tools	254
Log Analysis Tools	254
Password-Cracking Tools	254
Fuzzing and False Injection Tools	256
Wireless Tools	256
HTTP Interceptors	257
Local Exploitation Tools/Frameworks	257
Antivirus	257
Reverse Engineering Tools	257
Physical Security Tools	258
Summary	258
Exam Essentials	259
Review Questions	260
 Chapter 6	 Risk Management
	265
Risk Terminology	268
Identifying Vulnerabilities	270
Operational Risks	272
Risk in Business Models	273
Risk in External and Internal Influences	280
Adherence to Risk Management Frameworks	284
Enterprise Resilience	284
Risks with Data	285
The Risk Assessment Process	291
Asset Identification	291
Information Classification	293
Risk Assessment	294
Risk Analysis Options	299
Implementing Controls	301
Continuous Monitoring	302
Business Continuity Planning	303
Enterprise Security Architecture Frameworks and Governance	304
Best Practices for Risk Assessments	304
Summary	306

	Exam Essentials	306
	Resources	307
	Review Questions	309
Chapter 7	Policies, Procedures, and Incident Response	313
	A High-Level View of Documentation	316
	The Policy Development Process	317
	Policies and Procedures	318
	Business Documents Used to Support Security	323
	Documents and Controls Used for Sensitive Information	326
	Why Security?	326
	Personally Identifiable Information Controls	327
	Data Breaches	329
	Policies Used to Manage Employees	331
	Training and Awareness for Users	335
	Auditing Requirements and Frequency	336
	The Incident Response Framework	337
	Incident and Emergency Response	340
	Facilitate Incident Detection and Response	342
	Vulnerabilities Yet to Discover	342
	Incident Response Support Tools	342
	Severity of Incidents and Breaches	346
	Digital Forensics Tasks	346
	Summary	350
	Exam Essentials	351
	Review Questions	353
Chapter 8	Security Research and Analysis	357
	Applying Research Methods to Determine Industry	
	Trends and Impact on the Enterprise	361
	Performing Ongoing Research	361
	Best Practices	366
	New Technologies	369
	Situational Awareness	378
	Client-Side Attacks	379
	Knowledge of Current Vulnerabilities and Threats	382
	Research Security Implications of Emerging	
	Business Tools	387
	Global IA Industry Community	391
	Research Security Requirements for Contracts	396
	Analyze Scenarios to Secure the Enterprise	397
	Benchmarking and Baselining	398
	Prototyping and Testing Multiple Solutions	398
	Cost-Benefit Analysis	398

Analyze and Interpret Trend Data to Anticipate	
Cyber Defense Needs	399
Reviewing the Effectiveness of Existing Security Controls	400
Conducting Lessons Learned and After-Action Reviews	402
Reverse Engineering or Deconstructing Existing Solutions	403
Creation, Collection, and Analysis of Metrics	403
Analyzing Security Solutions to Ensure	
They Meet Business Needs	404
Using Judgment to Solve Difficult Problems	405
Summary	406
Exam Essentials	406
Review Questions	408

Chapter 9 Enterprise Security Integration 413

Integrate Enterprise Disciplines to Achieve Secure Solutions	417
Governance, Risk, and Compliance	419
Interpreting Security Requirements and Goals to	
Communicate with Stakeholders from Other Disciplines	421
Providing Objective Guidance and Impartial	
Recommendations to Staff and Senior Management	
on Security Processes and Controls	425
Establish Effective Collaboration within Teams	
to Implement Secure Solutions	427
Disciplines	430
Integrate Hosts, Storage, Networks, and Applications	
into a Secure Enterprise Architecture	433
Adapt Data Flow Security to Meet Changing	
Business Needs	436
Logical Deployment Diagram and Corresponding	
Physical Deployment Diagram of All Relevant Devices	438
Secure Infrastructure Design	438
Standards	439
Design Considerations during Mergers, Acquisitions,	
and Demergers/Divestitures	439
Technical Deployment Models (Outsourcing,	
Insourcing, Managed Services, Partnership)	440
Implementing Cryptographic Techniques	442
Security and Privacy Considerations of Storage	
Integration	442
In-House Developed vs. Commercial vs. Commercial	
Customized	443
Interoperability Issues	445
Security Implications of Integrating Enterprise Applications	447
Integrate Mobility Management	448
Containerization	448

	Mobile Management Techniques	449
	Signature and Application Concerns	450
	Whose Device Is It Anyway?	451
	Summary	452
	Exam Essentials	453
	Review Questions	454
Chapter 10	Security Controls for Communication and Collaboration	459
	Selecting the Appropriate Control to Secure	
	Communications and Collaboration Solutions	464
	Security of Unified Collaboration	464
	VoIP	473
	VoIP Implementation	475
	Trust Models and Remote Access	476
	Mobile Device Management	478
	Tethering	478
	Secure External Communications	479
	Secure Implementation of Collaboration Sites and Platforms	481
	Prioritizing Traffic with QoS	483
	Mobile Devices	484
	Integrate Advanced Authentication and Authorization	
	Technologies to Support Enterprise Objectives	488
	Authentication	489
	Federation and SAML	490
	Identity Proofing	491
	Identity Propagation	491
	Authorization	492
	SOAP	493
	Single Sign-On	494
	Attestation	495
	Certificate-Based Authentication	495
	Implement Security Activities across the Technology Life Cycle	497
	Systems Development Life Cycle	497
	Adapt Solutions to Address Emerging Threats and Security Trends	504
	Validating System Designs	507
	Integrate Security Controls for Mobile and Small Form Factor Devices	508
	Physical Security Tools for Security Assessment	511
	Summary	512
	Exam Essentials	512
	Review Questions	514

Appendix A	Answers to Review Questions	519
	Chapter 1: Cryptographic Tools and Techniques	520
	Chapter 2: Comprehensive Security Solutions	521
	Chapter 3: Securing Virtualized, Distributed and Shared Computing	522
	Chapter 4: Host Security	523
	Chapter 5: Application Security and Penetration Testing	524
	Chapter 6: Risk Management	526
	Chapter 7: Policies, Procedures, and Incident Response	527
	Chapter 8: Security Research and Analysis	528
	Chapter 9: Enterprise Security Integration	529
	Chapter 10: Security Controls for Communication and Collaboration	531
Appendix B	CASP+ Lab Manual	533
	What You'll Need	534
	Lab A1: Verifying a Baseline Security Configuration	537
	Lab A2: Introduction to a Protocol Analyzer	540
	Lab A3: Performing a Wireless Site Survey	543
	Lab A4: Using Windows Remote Access	544
	Connecting to the Remote Desktop PC	545
	Lab A5: Configuring a VPN Client	547
	Lab A6: Using the Windows Command-Line Interface (CLI)	549
	Lab A7: Cisco IOS Command-Line Basics	550
	Lab A8: Shopping for Wi-Fi Antennas	552
	Lab A9: Cloud Provisioning	554
	Lab A10: Introduction to Windows Command-Line Forensic Tools	555
	Lab A11: Introduction to Hashing Using a GUI	561
	Lab A12: Hashing from the Command Line	563
	Verifying File Integrity from a Command Line	563
	Verifying File Integrity on a Downloaded File	564
	Lab A13: Cracking Encrypted Passwords	565
	Lab A14: Threat Modeling	568
	Lab A15: Social Engineering	569
	Lab A16: Downloading, Verifying, and Installing a Virtual Environment	572
	Lab A17: Exploring Your Virtual Network	574
	Lab A18: Port Scanning	579
	Lab A19: Introduction to the Metasploit Framework	583
	Lab A20: Sniffing NETinVM Traffic with Wireshark	585
	Suggestions for Further Exploration of Security Topics	589
	<i>Index</i>	591

Table of Exercises

Exercise	2.1	Sniffing VoIP Traffic	60
Exercise	2.2	Spoofing MAC Addresses with SMAC	63
Exercise	2.3	Sniffing IPv4 with Wireshark	65
Exercise	2.4	Capturing a Ping Packet with Wireshark	69
Exercise	2.5	Capturing a TCP Header with Wireshark	71
Exercise	2.6	Using Men & Mice to Verify DNS Configuration	78
Exercise	2.7	Attempting a Zone Transfer	79
Exercise	3.1	What Services Should Be Moved to the Cloud?	109
Exercise	3.2	Identifying Risks and Issues with Cloud Computing	112
Exercise	3.3	Turning to the Cloud for Storage and Large File Transfer	117
Exercise	3.4	Creating a Virtual Machine	120
Exercise	3.5	Understanding Online Storage	133
Exercise	4.1	Reviewing and Assessing ACLs	151
Exercise	4.2	Configuring iptables	154
Exercise	4.3	Testing Your Antivirus Program	166
Exercise	4.4	Taking Control of a Router with Physical Access	173
Exercise	4.5	Running a Security Scanner to Identify Vulnerabilities	174
Exercise	4.6	Bypassing Command Shell Restrictions	175
Exercise	5.1	Identifying Testing Types at Your Organization	202
Exercise	5.2	Downloading and Running Kali Linux	243
Exercise	5.3	Performing Passive Reconnaissance on Your Company or Another Organization	245
Exercise	5.4	Performing TCP and UDP Port Scanning	248
Exercise	6.1	Tracking Vulnerabilities in Software	270
Exercise	6.2	Outsourcing Issues to Review	276
Exercise	6.3	Calculating Annualized Loss Expectancy	297
Exercise	7.1	Reviewing Security Policy	322
Exercise	7.2	Reviewing Documents	326
Exercise	7.3	Reviewing the Employee Termination Process	334
Exercise	7.4	Exploring Helix, a Well-Known Forensic Tool	350
Exercise	8.1	Using WinDump to Sniff Traffic	370
Exercise	8.2	Exploring the Nagios Tool	371
Exercise	8.3	Using Ophcrack	374

Exercise	8.4	Installing Cookie Cadger	380
Exercise	8.5	Identifying XSS Vulnerabilities	381
Exercise	9.1	Reviewing Your Company’s Acceptable Use Policy	424
Exercise	10.1	Eavesdropping on Web Conferences	465
Exercise	10.2	Sniffing Email with Wireshark.	471
Exercise	10.3	Sniffing VoIP with Cain & Abel	473

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