CompTIA®

CASP+

PRACTICE TESTS

Second Edition

EXAM CAS-004

Provides 1,000 practice questions covering all exam objectives.

Complements the CASP+ Study Guide, Fourth Edition, Exam CAS-004.

NADEAN H. TANNER

SYBEX®
A Wiley Brand

CASP+

Advanced Security
Practitioner Practice Tests
Second Edition

CASP+

Advanced Security Practitioner Practice Tests

Exam CAS-004

Second Edition

Nadean H. Tanner

SYBEX®
A Wiley Brand

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`.

73c99f3c5cb19301ed9de1524c40a1b8

Acknowledgments

About the Author

Nadean H. Tanner is the manager of Consulting – Education Services at FireEye/Mandiant, working most recently on building real-world cyber-range engagements to practice threat hunting and incident response. She has been in IT for more than 20 years and specifically in cybersecurity for over a decade. She holds over 30 industry certifications, including CompTIA CASP+, Security+, and (ISC)[2] CISSP.

Tanner has trained and consulted for Fortune 500 companies and the U.S. Department of Defense in cybersecurity, forensics, analysis, red/blue teaming, vulnerability management, and security awareness.

She is the author of *Cybersecurity Blue Team Toolkit*, published by Wiley in 2019, and *CASP+ Practice Tests: Exam CAS-003*, published by Sybex in 2020. She also was the technical editor for *CompTIA Security+ Study Guide: Exam SY0-601* (Sybex, 2021) and *CompTIA PenTest+ Study Guide: Exam PT0-002* (Sybex, 2021), both written by Mike Chapple and David Seidl.

In her spare time, Tanner enjoys speaking at technical conferences such as Black Hat, Wild West Hacking Fest, and OWASP events.

About the Technical Editor

Ryan Hendricks (CISSP, CEH, CASP+, Security+) has more than 16 years of cybersecurity and intelligence experience. His first venture started while working intelligence operations for the U.S. Navy and then continued in the government and private sector as an educator, facilitator, consultant, and adviser on a multitude of information technology and cybersecurity principles.

Hendricks holds many certifications covering hardware, networking, operating systems, and cybersecurity. He worked as a trainer for the U.S. Department of Defense, educating hundreds of students on everything from military communication systems to the CompTIA CASP+ and (ISC)[2] CISSP certifications.

Hendricks is a staff architect and manager at VMware. He currently supports all technical content creation for the VMware Carbon Black portfolio and additional VMware Security products. Additional responsibilities include developing labs, updating materials, piloting and expanding the certification programs, mentoring and managing the security technical content team, and educating anyone who is willing to learn. When not working, Hendricks tries to balance spending his time learning new security tools and attack techniques to feed his need for knowledge and playing video games with his kids.

Contents at a Glance

Contents

Introduction

CASP+ Advanced Security Practitioner Practice Tests is a companion volume to *CASP+ Study Guide*. If you're looking to test your knowledge before you take the CASP+ exam, this book will help you by providing a combination of 1,000 questions that cover the four CASP+ domains and by including easy-to-understand explanations of both right and wrong answers.

If you're just starting to prepare for the CASP+ exam, we highly recommend that you use *CASP+ Study Guide: Exam CAS-004* by Jeff T. Parker to help you learn about each of the domains covered by the CASP+ exam. Once you're ready to test your knowledge, use this book to help find places where you might need to read a chapter again and study more.

Because this is a companion to the CASP+ Study Guide, this book is designed to be similar to taking the CASP+ exam. It contains multipart scenarios as well as standard multiple-choice questions similar to those you will encounter on the certification exam.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

To submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

Chapter

1

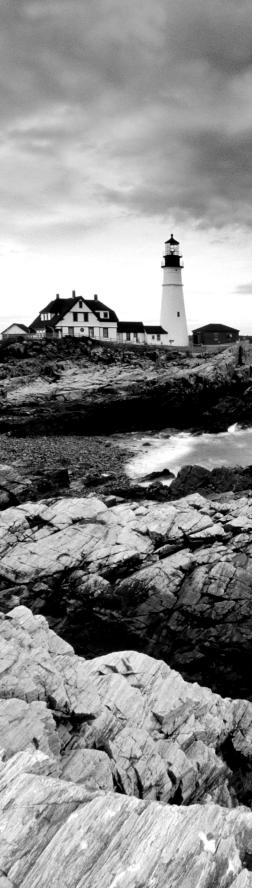# Security Architecture

---

THE CASP+ EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

✓ **Domain 1: Security Architecture**

- 1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.

  - Services

    - Load balancer

    - Intrusion detection system (IDS)/network intrusion detection system (NIDS)/wireless intrusion detection system (WIDS)

    - Intrusion prevention system (IPS)/network intrusion prevention system (NIPS)/wireless intrusion prevention system (WIPS)

    - Web application firewall (WAF)

    - Network access control (NAC)

    - Virtual private network (VPN)

    - Domain Name System Security Extensions (DNSSEC)

    - Firewall/unified threat management (UTM)/next-generation firewall (NGFW)

    - Network address translation (NAT) gateway

    - Internet gateway

    - Forward/transparent proxy

    - Reverse proxy

    - Distributed denial-of-service (DDoS) protection

    - Routers

    - Mail security

    - Application programming interface (API) gateway/Extensible Markup Language (XML) gateway

- Traffic mirroring
- Switched port analyzer (SPAN) ports
- Port mirroring
- Virtual private cloud (VPC)
- Network tap
- Sensors
- Security information and event management (SIEM)
- File integrity monitoring (FIM)
- Simple Network Management Protocol (SNMP) traps
- NetFlow
- Data loss prevention (DLP)
- Antivirus
- Segmentation
  - Microsegmentation
  - Local area network (LAN)/virtual local area network (VLAN)
  - Jump box
  - Screened subnet
  - Data zones
  - Staging environments
  - Guest environments
  - VPC/virtual network (VNET)
  - Availability zone
  - NAC lists
  - Policies/security groups
  - Regions
  - Access control lists (ACLs)
  - Peer-to-peer
  - Air gap

- Deperimeterization/zero trust
    - Cloud
    - Remote work
    - Mobile
    - Outsourcing and contracting
    - Wireless/radio frequency (RF) networks
  - Merging of networks from various organizations
    - Peering
    - Cloud to on premises
    - Data sensitivity levels
    - Mergers and acquisitions
    - Cross-domain
    - Federation
    - Directory services
  - Software-defined networking (SDN)
    - Open SDN
    - Hybrid SDN
    - SDN overlay
- 1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.
  - Scalability
    - Vertically
    - Horizontally
  - Resiliency
    - High availability
    - Diversity/heterogeneity
    - Course of action orchestration
    - Distributed allocation
    - Redundancy
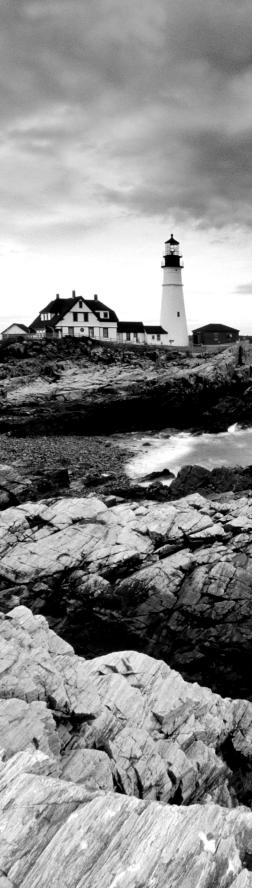   - Replication
    - Clustering

- Automation
    - Autoscaling
    - Security Orchestration, Automation and Response (SOAR)
    - Bootstrapping
  - Performance
  - Containerization
  - Virtualization
  - Content delivery network
  - Caching
- 1.3 Given a scenario, integrate software applications securely into an enterprise architecture.
  - Baseline and templates
    - Secure design patterns/types of web technologies
    - Storage design patterns
    - Container APIs
    - Secure coding standards
    - Application vetting processes
    - API management
    - Middleware
  - Software assurance
    - Sandboxing/development environment
    - Validating third-party libraries
    - Defined DevOps pipeline
    - Code signing
    - Interactive application security testing (IAST) vs. dynamic application security testing (DAST) vs. static application security testing (SAST)
  - Considerations of integrating enterprise applications
    - Customer relationship management (CRM)

- Enterprise resource planning (ERP)
- Configuration management database (CMDB)
- Content management system (CMS)
- Integration enablers
- Directory services
- Domain name system (DNS)
- Service-oriented architecture (SOA)
- Enterprise service bus (ESB)
- Integrating security into development life cycle
  - Formal methods
  - Requirements
  - Fielding
  - Insertions and upgrades
  - Disposal and reuse
  - Testing
  - Regression
  - Unit testing
  - Integration testing
  - Development approaches
  - SecDevOps
  - Agile
  - Waterfall
  - Spiral
  - Versioning
  - Continuous integration/continuous delivery (CI/CD) pipelines
  - Best practices
  - Open Web Application Security Project (OWASP)
  - Proper Hypertext Transfer Protocol (HTTP) headers

- 1.4 Given a scenario, implement data security techniques for securing enterprise architecture.
    - Data loss prevention
        - Blocking use of external media
        - Print blocking
        - Remote Desktop Protocol (RDP) blocking
        - Clipboard privacy controls
        - Restricted virtual desktop infrastructure (VDI) implementation
        - Data classification blocking
    - Data loss detection
        - Watermarking
        - Digital rights management (DRM)
        - Network traffic decryption/deep packet inspection
        - Network traffic analysis
    - Data classification, labeling, and tagging
        - Metadata/attributes
    - Obfuscation
        - Tokenization
        - Scrubbing
        - Masking
    - Anonymization
    - Encrypted vs. unencrypted
    - Data life cycle
        - Create
        - Use
        - Share
        - Store
        - Archive
        - Destroy

- Data inventory and mapping
- Data integrity management
- Data storage, backup, and recovery
  - Redundant array of inexpensive disks (RAID)
- 1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.
  - Credential management
    - Password repository application
    - End-user password storage
    - On premises vs. cloud repository
    - Hardware key manager
    - Privileged access management
  - Password policies
    - Complexity
    - Length
    - Character classes
    - History
    - Maximum/minimum age
    - Auditing
    - Reversable encryption
  - Federation
    - Transitive trust
    - OpenID
    - Security Assertion Markup Language (SAML)
    - Shibboleth
  - Access control
    - Mandatory access control (MAC)
    - Discretionary access control (DAC)
    - Role-based access control