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

Table of Contents

- Cover
- Title Page
- Copyright
- Dedication
- Acknowledgments
- About the Author
- About the Technical Editor
- Introduction
  - How to Contact the Publisher
- Chapter 1: Security Architecture
- Chapter 2: Security Operations
- Chapter 3: Security Engineering and Cryptography
- Chapter 4: Governance, Risk, and Compliance
- Chapter 5: Practice Test 1
- Chapter 6: Practice Test 2
- Appendix: Answers to Review Questions
  - Chapter 1: Security Architecture
  - Chapter 2: Security Operations
  - Chapter 3: Security Engineering and Cryptography
  - Chapter 4: Governance, Risk, and Compliance
  - Chapter 5: Practice Test 1
  - Chapter 6: Practice Test 2
- Index
- End User License Agreement

CASP+
Advanced Security Practitioner Practice Tests

Exam CAS-004

Second Edition

Nadean H. Tanner


SYBEX
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

ISBN: 978-1-119-81305-7

ISBN: 978-1-119-81307-1 (ebk)

ISBN: 978-1-119-81306-4 (ebk)

Library of Congress Control Number: 2021938732

73c99f3c5cb19301ed9de1524c40a1b8

Acknowledgments

To my husband, no one I'd rather quarantine with.

To my children, who will never read this book.

To Kenyon Brown, for trusting me to do this again.

To Kelly Talbot, for gently reminding me of deadlines.

To Ryan Hendricks, your turn!

—Nadean H. Tanner

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.

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
    - Rule-based access control
    - Attribute-based access control
- Protocols
    - Remote Authentication Dial-in User Server (RADIUS)
    - Terminal Access Controller Access Control System (TACACS)
    - Diameter
    - Lightweight Directory Access Protocol (LDAP)
    - Kerberos

        - OAuth
        - 802.1X
        - Extensible Authentication Protocol (EAP)
    - Multifactor authentication (MFA)
        - Two-factor authentication (2FA)
        - 2-Step Verification
        - In-band
        - Out-of-band
    - One-time password (OTP)
        - HMAC-based one-time password (HOTP)
        - Time-based one-time password (TOTP)
    - Hardware root of trust
    - Single sign-on (SSO)
    - JavaScript Object Notation (JSON) web token (JWT)
    - Attestation and identity proofing
- 1.6 Given a set of requirements, implement secure cloud and virtualization solutions.
    - Virtualization strategies
        - Type 1 vs. Type 2 hypervisors
        - Containers
        - Emulation
        - Application virtualization
        - VDI
    - Provisioning and deprovisioning
    - Middleware

- Metadata and tags
- Deployment models and considerations
  - Business directives
  - Cost
  - Scalability
  - Resources
  - Location
  - Data protection
  - Cloud deployment models
  - Private
  - Public
  - Hybrid
  - Community
- Hosting models
  - Multitenant
  - Single-tenant
- Service models
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
  - Infrastructure as a service (IaaS)
- Cloud provider limitations
  - Internet Protocol (IP) address scheme
  - VPC peering
- Extending appropriate on-premises controls
- Storage models

        - Object storage/file-based storage
        - Database storage
        - Block storage
        - Blob storage
        - Key-value pairs
- 1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.
    - Privacy and confidentiality requirements
    - Integrity requirements
    - Non-repudiation
    - Compliance and policy requirements
    - Common cryptography use cases
        - Data at rest
        - Data in transit
        - Data in process/data in use
        - Protection of web services
        - Embedded systems
        - Key escrow/management
        - Mobile security
        - Secure authentication
        - Smart card
    - Common PKI use cases
        - Web services
        - Email
        - Code signing

        - Federation
        - Trust models
        - VPN
        - Enterprise and security automation/orchestration
- 1.8 Explain the impact of emerging technologies on enterprise security and privacy.
    - Artificial intelligence
    - Machine learning
    - Quantum computing
    - Blockchain
    - Homomorphic encryption
        - Private information retrieval
        - Secure function evaluation
        - Private function evaluation
    - Secure multiparty computation
    - Distributed consensus
    - Big Data
    - Virtual/augmented reality
    - 3D printing
    - Passwordless authentication
    - Nano technology
    - Deep learning
        - Natural language processing
        - Deep fakes
    - Biometric impersonation

1. Your organization experienced a security event that led to the loss and disruption of services. You were chosen to investigate the disruption to prevent the risk of it happening again. What is this process called?
   A. Incident management
   B. Forensic tasks
   C. Mandatory vacation
   D. Job rotation
2. Brett is a new CISO, and he is evaluating different controls for availability. Which set of controls should he choose?
   A. RAID 1, classification of data, and load balancing
   B. Digital signatures, encryption, and hashes
   C. Steganography, ACLs, and vulnerability management
   D. Checksums, DOS attacks, and RAID 0
3. Charles has received final documentation from a compliance audit. The report suggested his organization should implement a complementary security tool to work with the firewall to detect any attempt at scanning. Which device does Charles choose?
   A. RAS
   B. PBX
   C. IDS
   D. DDT
4. Nicole is the security administrator for a large governmental agency. She has implemented port

security, restricted network traffic, and installed NIDS, firewalls, and spam filters. She thinks the network is secure. Now she wants to focus on endpoint security. What is the most comprehensive plan for her to follow?

A. Antimalware/virus/spyware, host-based firewall, and MFA

B. Antivirus/spam, host-based IDS, and TFA

C. Antimalware/virus, host-based IDS, and biometrics

D. Antivirus/spam, host-based IDS, and SSO

5. Sally's CISO asked her to recommend an intrusion system to recognize intrusions traversing the network and send email alerts to the IT staff when one is detected. What type of intrusion system does the CISO want?

A. HIDS

B. NIDS

C. HIPS

D. NIPS

6. Kenneth is the CISO of an engineering organization. He asked the security department to recommend a system to be placed on business-critical servers to detect and stop intrusions. Which of the following will meet the CISO's requirement?

A. HIPS

B. NIDS

C. HIDS

D. NIPS

7. Paul's company has discovered that some of his organization's employees are using personal devices,

including cell phones, within highly secure areas. The CISO wants to know which employees are violating this policy. Which of the following devices can inform the CISO who is violating this policy?

A. DLP

B. WIDS

C. NIPS

D. Firewall

8. Suzette's company discovered that some of her organization's employees are copying corporate documents to Microsoft blob cloud drives outside the control of the company. She has been instructed to stop this practice from occurring. Which of the following can stop this practice from happening?

A. DLP

B. NIDS

C. NIPS

D. Firewall

9. Troy must decide about his organization's file integrity monitoring (FIM) monitoring. Standalone FIM generally means file analysis only. Another option is to integrate it with the host so that Troy can detect threats in other areas, such a system memory or an I/O. For the integration, which of the following does Troy need to use?

A. HIDS

B. ADVFIM

C. NIDS

D. Change management

10. Lisa is building a network intrusion detection system (NIDS). What can an NIDS do with encrypted network traffic?

    A. Look for viruses

    B. Examine contents of email

    C. Bypass VPN

    D. Nothing

11. What system is used to collect and analyze data logs from various network devices and to report detected security events?

    A. Syslog server

    B. NIPS

    C. WIPS

    D. SIEM system

12. The IT department decided to implement a security appliance in front of their web servers to inspect HTTP/HTTPS/SOAP traffic for malicious activity. Which of the following is the *best* solution to use?

    A. Screened host firewall

    B. Packet filter firewall

    C. DMZ

    D. WAF

13. A security audit was conducted for your organization. It found that a computer plugged into any Ethernet port in its shipping facility was able to access network resources without authentication. You are directed to fix this security issue. Which standard, if implemented, could resolve this issue?

    A. 802.1x