CompTIA®

CySA+

PRACTICE TESTS

Second Edition

EXAM CS0-002

Provides 1,000 practice questions covering all the exam objectives.

Complements the *CompTIA CySA+ Study Guide, Second Edition*, Exam CS0-002.

MIKE CHAPPLE
DAVID SEIDL

SYBEX®
A Wiley Brand

CompTIA®

Cybersecurity Analyst (CySA+™) Practice Tests

Exam CS0-002

Second Edition

CompTIA®

Cybersecurity Analyst (CySA+™) Practice Tests

Exam CS0-002

Second Edition

Mike Chapple

David Seidl

SYBEX®
A Wiley Brand

Published simultaneously in Canada

ISBN: 978-1-119-68379-7
ISBN: 978-1-119-68392-6 (ebk.)
ISBN: 978-1-119-68404-6 (ebk.)

Library of Congress Control Number: 2020938566

For Renee, the most patient and caring person I know. Thank you for being the heart of our family.
—MJC

This book is dedicated to my longtime friend Amanda Hanover, who always combined unlimited curiosity with equally infinite numbers of questions about security topics. Amanda lost her fight with mental health struggles in 2019, but you, our reader, should know that there is support out there. Mental health challenges are a struggle that many in the security community face, and community support exists for those who need it. Visit `www.mentalhealthhackers.org` *to find mental health activities at security conferences in your area, as well as resources and links to other resources. You are not alone.*

And Amanda—here are a thousand more security questions for you. Your friend, David
—DAS

Acknowledgments

The authors would like to thank the many people who made this book possible. Kenyon Brown at Wiley has been a wonderful partner through many books over the years. Carole Jelen, our agent, worked on a myriad of logistic details and handled the business side of the book with her usual grace and commitment to excellence. Chris Crayton, our technical editor, pointed out many opportunities to improve our work and deliver a high-quality final product. Kezia Endsley served as developmental editor and managed the project smoothly. Thank you to Runzhi "Tom" Song, Mike's research assistant at Notre Dame, who spent hours proofreading our final copy. Many other people we'll never meet worked behind the scenes to make this book a success.

About the Authors

Mike Chapple, PhD, CISSP, is an author of the best-selling *CySA+ Study Guide* and *CISSP (ISC)² Certified Information Systems Security Professional Official Study Guide*, now in its eighth edition. He is an information security professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as teaching professor of IT, analytics, and operations at the University of Notre Dame, where he teaches courses focused on cybersecurity and business analytics.

Before returning to Notre Dame, Mike served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active duty intelligence officer in the U.S. Air Force.

Mike earned both his BS and PhD degrees from Notre Dame in computer science and engineering. He also holds an MS in computer science from the University of Idaho and an MBA from Auburn University.

David Seidl is the Vice President for Information Technology and CIO at Miami University. During his IT career, he has served in a variety of technical and information security roles, including serving at the Senior Director for Campus Technology Services at the University of Notre Dame, where he co-led Notre Dame's move to the cloud and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and service. He also served as Notre Dame's Director of Information Security and led Notre Dame's information security program. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business and has written books on security certification and cyberwarfare, including co-authoring *CISSP (ISC)² Official Practice Tests* (Sybex 2018) as well as the previous editions of both this book and the companion *CompTIA CySA+ Practice Tests: Exam CS0-001*.

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as CISSP, CySA+, Pentest+, GPEN, and GCIH certifications.

About the Technical Editor

Chris Crayton, MCSE, CISSP, CASP, CySA+, A+, N+, S+, is a technical consultant, trainer, author and industry leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He has also been recognized with many professional and teaching awards.

Contents at a Glance

Contents

Introduction

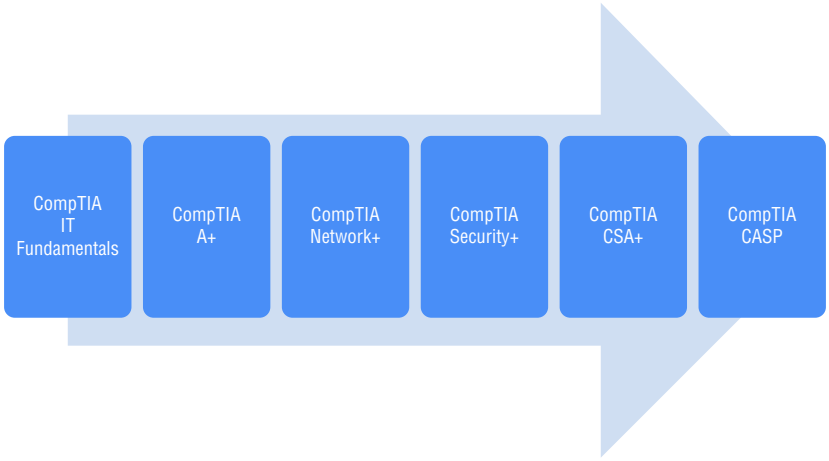
CompTIA CySA+ (Cybersecurity Analyst) Practice Tests, Second Edition is a companion volume to the *CompTIA CySA+ Study Guide, Second Edition* (Sybex, 2020, Chapple/Seidl). If you're looking to test your knowledge before you take the CySA+ exam, this book will help you by providing a combination of 1,000 questions that cover the CySA+ domains and easy-to-understand explanations of both right and wrong answers.

If you're just starting to prepare for the CySA+ exam, we highly recommend that you use the *Cybersecurity Analyst+ (CySA+) Study Guide, Second Edition* to help you learn about each of the domains covered by the CySA+ exam. Once you're ready to test your knowledge, use this book to help find places where you may need to study more or to practice for the exam itself.

Since this is a companion to the *CySA+ Study Guide*, this book is designed to be similar to taking the CySA+ exam. It contains multipart scenarios as well as standard multiple-choice questions similar to those you may encounter in the certification exam itself. The book itself is broken up into seven chapters: five domain-centric chapters with questions about each domain, and two chapters that contain 85-question practice tests to simulate taking the CySA+ exam itself.

CompTIA

CompTIA is a nonprofit trade organization that offers certification in a variety of IT areas, ranging from the skills that a PC support technician needs, which are covered in the A+ exam, to advanced certifications like the CompTIA Advanced Security Practitioner, or CASP certification. CompTIA recommends that practitioners follow a cybersecurity career path as shown here:



The Cybersecurity Analyst+ exam is a more advanced exam, intended for professionals with hands-on experience and who possess the knowledge covered by the prior exams.

CompTIA certifications are ISO and ANSI accredited, and they are used throughout multiple industries as a measure of technical skill and knowledge. In addition, CompTIA certifications, including the CySA+, the Security+ and the CASP certifications, have been approved by the U.S. government as Information Assurance baseline certifications and are included in the State Department's Skills Incentive Program.

The Cybersecurity Analyst+ Exam

The Cybersecurity Analyst+ exam, which CompTIA refers to as CySA+, is designed to be a vendor-neutral certification for cybersecurity, threat, and vulnerability analysts. The CySA+ certification is designed for security analysts and engineers as well as security operations center (SOC) staff, vulnerability analysts, and threat intelligence analysts. It focuses on security analytics and practical use of security tools in real-world scenarios. It covers five major domains: Threat and Vulnerability Management, Software and Systems Security, Security Operations and Monitoring, Incident Response, and Compliance and Assessment. These five areas include a range of topics, from reconnaissance to incident response and forensics, while focusing heavily on scenario-based learning.

The CySA+ exam fits between the entry-level Security+ exam and the CompTIA Advanced Security Practitioner (CASP) certification, providing a mid-career certification for those who are seeking the next step in their certification and career path.

The CySA+ exam is conducted in a format that CompTIA calls "performance-based assessment." This means that the exam uses hands-on simulations using actual security tools and scenarios to perform tasks that match those found in the daily work of a security practitioner. Exam questions may include multiple types of questions such as multiple-choice, fill-in-the-blank, multiple-response, drag-and-drop, and image-based problems.

CompTIA recommends that test takers have four years of information security–related experience before taking this exam. The exam costs $359 in the United States, with roughly equivalent prices in other locations around the globe. More details about the CySA+ exam and how to take it can be found at `certification.comptia.org/certifications/cybersecurity-analyst`.

Study and Exam Preparation Tips

We recommend you use this book in conjunction with the *Cybersecurity Analyst+ (CySA+) Study Guide, Second Edition*. Read through chapters in the study guide and then try your hand at the practice questions associated with each domain in this book.

You should also keep in mind that the CySA+ certification is designed to test practical experience, so you should also make sure that you get some hands-on time with the

security tools covered on the exam. CompTIA recommends the use of NetWars-style simulations, penetration testing and defensive cybersecurity simulations, and incident response training to prepare for the CySA+.

Additional resources for hands-on exercises include the following:

- Exploit-Exercises.com provides virtual machines, documentation, and challenges covering a wide range of security issues at `exploit-exercises.lains.space`.
- Hacking-Lab provides capture-the-flag (CTF) exercises in a variety of fields at `www.hacking-lab.com/index.html`.
- PentesterLab provides a subscription-based access to penetration testing exercises at `www.pentesterlab.com/exercises/`.
- The InfoSec Institute provides online capture-the-flag activities with bounties for written explanations of successful hacks at `ctf.infosecinstitute.com`.

Since the exam uses scenario-based learning, expect the questions to involve analysis and thought, rather than relying on simple memorization. As you might expect, it is impossible to replicate that experience in a book, so the questions here are intended to help you be confident that you know the topic well enough to think through hands-on exercises.

Taking the Exam

Once you are fully prepared to take the exam, you can visit the CompTIA website to purchase your exam voucher:

`www.comptiastore.com/Articles.asp?ID=265&category=vouchers`

CompTIA partners with Pearson VUE's testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your ZIP code, while non-U.S. test takers may find it easier to enter their city and country. You can search for a test center near you at the Pearson Vue website, where you will need to navigate to "Find a test center":

`www.pearsonvue.com/comptia/`

Now that you know where you'd like to take the exam, simply set up a Pearson VUE testing account and schedule an exam:

`www.comptia.org/testing/testing-options/take-in-person-exam`

On the day of the test, bring two forms of identification, and make sure to show up with plenty of time before the exam starts. Remember that you will not be able to take your notes, electronic devices (including smartphones and watches), or other materials in with you.

After the Cybersecurity Analyst+ Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam.

Maintaining Your Certification

CompTIA certifications must be renewed on a periodic basis. To renew your certification, you can either pass the most current version of the exam, earn a qualifying higher-level CompTIA or industry certification, or complete sufficient continuing education activities to earn enough continuing education units (CEUs) to renew it.

CompTIA provides information on renewals via their website at

`www.comptia.org/continuing-education`

When you sign up to renew your certification, you will be asked to agree to the CE program's Code of Ethics, to pay a renewal fee, and to submit the materials required for your chosen renewal method.

A full list of the industry certifications you can use to acquire CEUs toward renewing the CySA+ can be found at

`www.comptia.org/continuing-education/choose/renew-with-a-single-activity/earn-a-higher-level-comptia-certification`

Using This Book to Practice

This book is composed of seven chapters. Each of the first five chapters covers a domain, with a variety of questions that can help you test your knowledge of real-world, scenario, and best practices–based security knowledge. The final two chapters are complete practice exams that can serve as timed practice tests to help determine whether you're ready for the CySA+ exam.

We recommend taking the first practice exam to help identify where you may need to spend more study time and then using the domain-specific chapters to test your domain knowledge where it is weak. Once you're ready, take the second practice exam to make sure you've covered all the material and are ready to attempt the CySA+ exam.

As you work through questions in this book, you will encounter tools and technology that you may not be familiar with. If you find that you are facing a consistent gap or that a domain is particularly challenging, we recommend spending some time with books and materials that tackle that domain in depth. This can help you fill in gaps and help you be more prepared for the exam.

Objectives Map for CompTIA CySA+ (Cybersecurity Analyst) Exam CS0-002

The following objective map for the CompTIA CySA+ (Cybersecurity Analyst) certification exam will enable you to find where each objective is covered in the book.

Objectives Map

Objective	Chapter
1.0 Threat and Vulnerability Management	
1.1 Explain the importance of threat data and intelligence.	Chapter 1
1.2 Given a scenario, utilize threat intelligence to support organizational security.	Chapter 1
1.3 Given a scenario, perform vulnerability management activities.	Chapter 1
1.4 Given a scenario, analyze the output from common vulnerability assessment tools.	Chapter 1
1.5 Explain the threats and vulnerabilities associated with specialized technology.	Chapter 1
1.6 Explain the threats and vulnerabilities associated with operating in the cloud.	Chapter 1
1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.	Chapter 1
2.0 Software and Systems Security	
2.1 Given a scenario, apply security solutions for infrastructure management.	Chapter 2
2.2 Explain software assurance best practices.	Chapter 2
2.3 Explain hardware assurance best practices.	Chapter 2
3.0 Security Operations and Monitoring	
3.1 Given a scenario, analyze data as part of security monitoring activities.	Chapter 3
3.2 Given a scenario, implement configuration changes to existing controls to improve security.	Chapter 3
3.3 Explain the importance of proactive threat hunting.	Chapter 3
3.4 Compare and contrast automation concepts and technologies.	Chapter 3
4.0 Incident Response	
4.1 Explain the importance of the incident response process.	Chapter 4
4.2 Given a scenario, apply the appropriate incident response procedure.	Chapter 4
4.3 Given an incident, analyze potential indicators of compromise.	Chapter 4
4.4 Given a scenario, utilize basic digital forensic techniques.	Chapter 4
5.0 Compliance and Assessment	
5.1 Understand the importance of data privacy and protection.	Chapter 5
5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.	Chapter 5
5.3 Explain the importance of frameworks, policies, procedures, and controls.	Chapter 5

Chapter 1

Domain 1.0: Threat and Vulnerability Management

EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **1.1 Explain the importance of threat data and intelligence.**

- Intelligence sources
- Confidence levels
- Indicator management
- Threat classification
- Threat actors
- Intelligence cycle
- Commodity malware
- Information sharing and analysis communities

✓ **1.2 Given a scenario, utilize threat intelligence to support organizational security.**

- Attack frameworks
- Threat research
- Threat modeling methodologies
- Threat intelligence sharing with supported functions

✓ **1.3 Given a scenario, perform vulnerability management activities.**

- Vulnerability identification
- Validation
- Remediation/mitigation
- Scanning parameters and criteria
- Inhibitors to remediation

✓ **1.4 Given a scenario, analyze the output from common vulnerability assessment tools.**

- Web application scanner

- Infrastructure vulnerability scanner
- Software assessment tools and techniques
- Enumeration
- Wireless assessment tools
- Cloud infrastructure assessment tools

✓ **1.5 Explain the threats and vulnerabilities associated with specialized technology.**

- Mobile
- Internet of Things (IoT)
- Embedded
- Real-time operating system (RTOS)
- System-on-Chip (SoC)
- Field programmable gate array (FPGA)
- Physical access control
- Building automation systems
- Vehicles and drones
- Workflow and process automation systems
- Industrial control systems (ICS)
- Supervisory control and data acquisition (SCADA)

✓ **1.6 Explain the threats and vulnerabilities associated with operating in the cloud.**

- Cloud service models
- Cloud deployment models
- Function as a service (FaaS)/serverless architecture
- Infrastructure as code (IaC)
- Insecure application programming interface (API)
- Improper key management
- Unprotected storage
- Logging and monitoring

✓ **1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.**

- Attack types
- Vulnerabilities

1. Olivia is considering potential sources for threat intelligence information that she might incorporate into her security program. Which one of the following sources is most likely to be available without a subscription fee?
   - **A.** Vulnerability feeds
   - **B.** Open source
   - **C.** Closed source
   - **D.** Proprietary

2. During the reconnaissance stage of a penetration test, Cynthia needs to gather information about the target organization's network infrastructure without causing an IPS to alert the target to her information gathering. Which of the following is her best option?
   - **A.** Perform a DNS brute-force attack.
   - **B.** Use an nmap ping sweep.
   - **C.** Perform a DNS zone transfer.
   - **D.** Use an nmap stealth scan.

3. Roger is evaluating threat intelligence information sources and finds that one source results in quite a few false positive alerts. This lowers his confidence level in the source. What criteria for intelligence is not being met by this source?
   - **A.** Timeliness
   - **B.** Expense
   - **C.** Relevance
   - **D.** Accuracy

4. What markup language provides a standard mechanism for describing attack patterns, malware, threat actors, and tools?
   - **A.** STIX
   - **B.** TAXII
   - **C.** XML
   - **D.** OpenIOC

5. A port scan of a remote system shows that port 3306 is open on a remote database server. What database is the server most likely running?
   - **A.** Oracle
   - **B.** Postgres
   - **C.** MySQL
   - **D.** Microsoft SQL

6. Brad is working on a threat classification exercise, analyzing known threats and assessing the possibility of unknown threats. Which one of the following threat actors is most likely to be associated with an advanced persistent threat (APT)?
   - **A.** Hacktivist
   - **B.** Nation-state

C. Insider

D. Organized crime

7. During a port scan of her network, Cynthia discovers a workstation that shows the following ports open. What should her next action be?

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-26 19:25 EDT
Nmap scan report for deptsrv (192.168.2.22)
Host is up (0.0058s latency).
Not shown: 65524 closed ports
PORT      STATE    SERVICE
80/tcp    open     http
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
3389/tcp  open     ms-wbt-server
7680/tcp  open     unknown
49677/tcp open     unknown
MAC Address: AD:5F:F4:7B:4B:7D (Intel Corporation)

Nmap done: 1 IP address (1 host up) scanned in 121.29 seconds
```

A. Determine the reason for the ports being open.

B. Investigate the potentially compromised workstation.

C. Run a vulnerability scan to identify vulnerable services.

D. Reenable the workstation's local host firewall.

8. Charles is working with leaders of his organization to determine the types of information that should be gathered in his new threat intelligence program. In what phase of the intelligence cycle is he participating?

A. Dissemination

B. Feedback

C. Analysis

D. Requirements

9. As Charles develops his threat intelligence program, he creates and shares threat reports with relevant technologists and leaders. What phase of the intelligence cycle is now occurring?

A. Dissemination

B. Feedback

C. Collection

D. Requirements

10. What term is used to describe the groups of related organizations who pool resources to share cybersecurity threat information and analyses?

A. SOC

B. ISAC

C. CERT

D. CIRT

11. Which one of the following threats is the most pervasive in modern computing environments?

A. Zero-day attacks

B. Advanced persistent threats

C. Commodity malware

D. Insider threats

12. Singh incorporated the Cisco Talos tool into his organization's threat intelligence program. He uses it to automatically look up information about the past activity of IP addresses sending email to his mail servers. What term best describes this intelligence source?

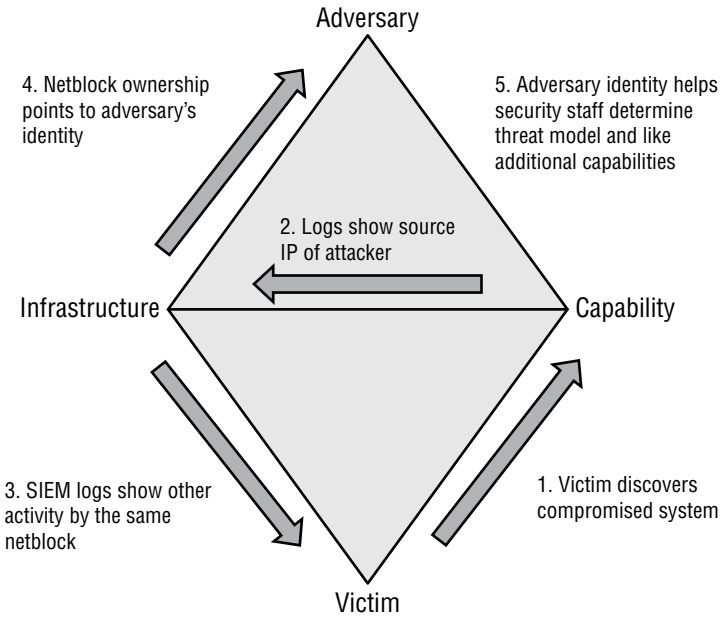
A. Open source

B. Behavioral

C. Reputational

D. Indicator of compromise

13. Consider the threat modeling analysis shown here. What attack framework was used to develop this analysis?



A. ATT&CK

B. Cyber Kill Chain

C. STRIDE

D. Diamond

14. Jamal is assessing the risk to his organization from their planned use of AWS Lambda, a serverless computing service that allows developers to write code and execute functions directly on the cloud platform. What cloud tier best describes this service?

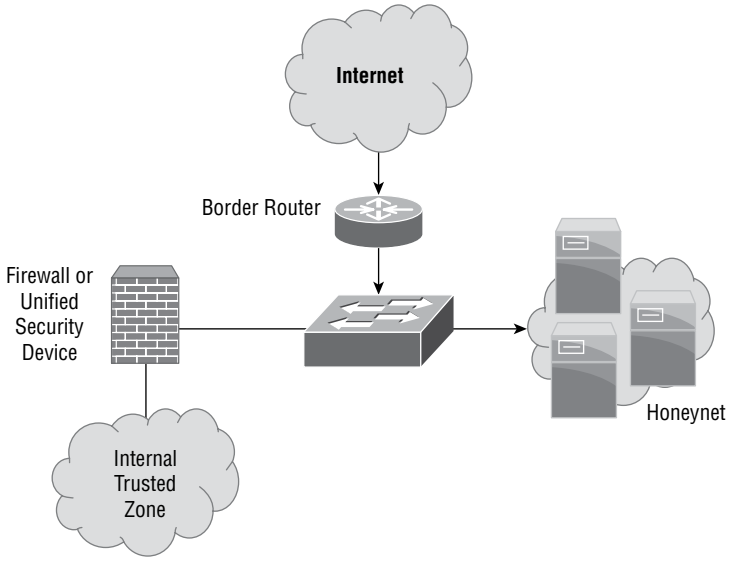
A. SaaS

B. PaaS

C. IaaS

D. FaaS

15. Lauren's honeynet, shown here, is configured to use a segment of unused network space that has no legitimate servers in it. What type of threats is this design particularly useful for detecting?



A. Zero-day attacks

B. SQL injection

C. Network scans

D. DDoS attacks

16. Nara is concerned about the risk of attackers conducting a brute-force attack against her organization. Which one of the following factors is Nara most likely to be able to control?

A. Attack vector

B. Adversary capability