Sean-Philip Oriyano

CEH™

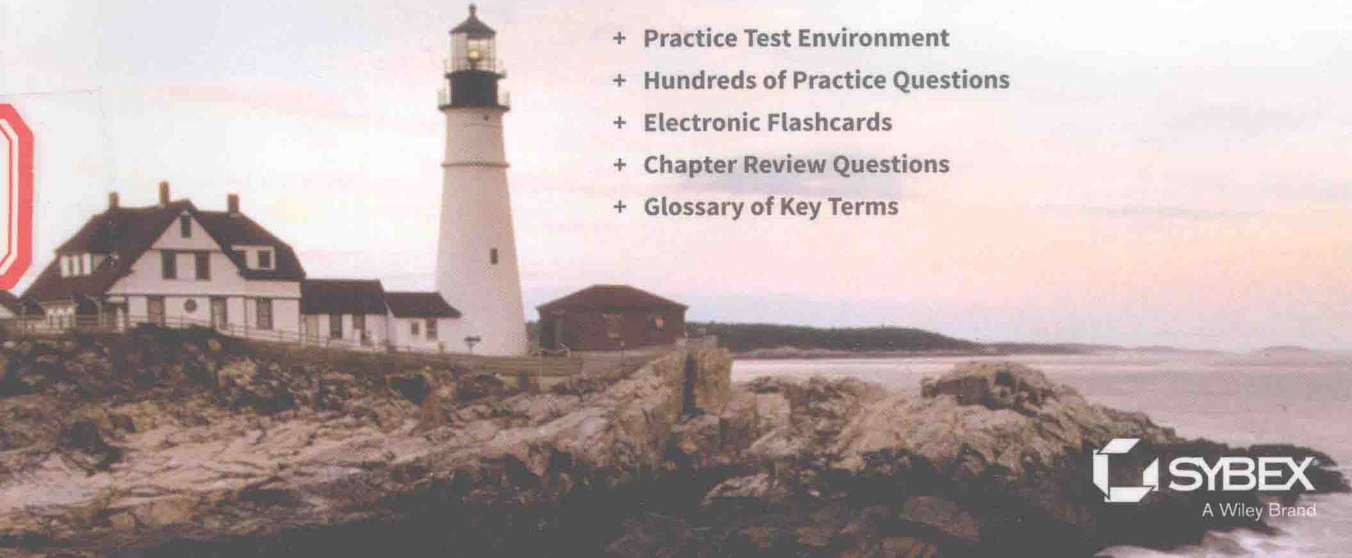
Certified Ethical Hacker Version 8

STUDY GUIDE

EXAM 312-50/EC0-350

Includes Real-World Scenarios, Hands-On Exercises, and Access to Exam Prep Software Featuring:

- **Practice Test Environment**
- **Hundreds of Practice Questions**
- **Electronic Flashcards**
- **Chapter Review Questions**
- **Glossary of Key Terms**

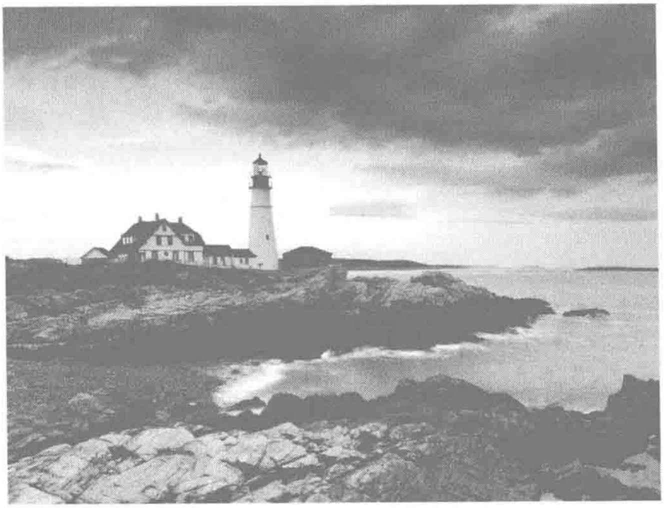


SYBEX
A Wiley Brand

CEHv8

Certified Ethical Hacker Version 8

Study Guide



Sean-Philip Oriyano

SYBEX
A Wiley Brand

Senior Acquisitions Editor: Jeff Kellum
Development Editor: Richard Mateosian
Technical Editors: Albert Whale and Robert Burke
Production Editor: Dassi Zeidel
Copy Editors: Liz Welch and Tiffany Taylor
Editorial Manager: Pete Gaughan
Vice President and Executive Group Publisher: Richard Swadley
Associate Publisher: Chris Webb
Media Project Manager I: Laura Moss-Hollister
Media Associate Producer: Marilyn Hummel
Media Quality Assurance: Doug Kuhn
Book Designer: Judy Fung
Proofreader: Sarah Kaikini, Word One New York
Indexer: Ted Laux
Project Coordinator, Cover: Patrick Redmond
Cover Designer: Wiley
Cover Image: ©Getty Images Inc./Jeremy Woodhouse

Published simultaneously in Canada

ISBN: 978-1-118-64767-7

ISBN: 978-1-118-76332-2 (ebk.)

ISBN: 978-1-118-98928-9 (ebk.)

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.

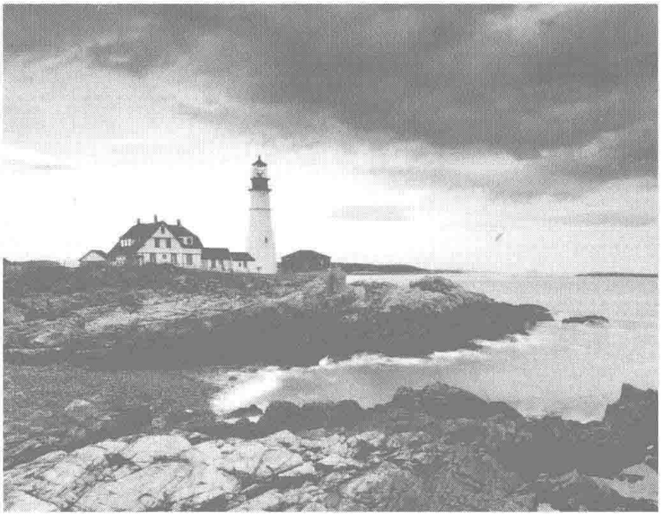
Library of Congress Control Number: 2014931949.

10 9 8 7 6 5 4 3

CEHv8

Certified Ethical Hacker Version 8

Study Guide



Dear Reader,

Thank you for choosing *CEHv8: Certified Ethical Hacker Version 8 Study Guide*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an e-mail at `contactus@sybex.com`. If you think you've found a technical error in this book, please visit `http:sybex.custhelp.com`. Customer feedback is critical to our efforts at Sybex.

Best regards,

Chris Webb
Associate Publisher
Sybex, an Imprint of Wiley

Acknowledgments

First, I would like to send a big thanks out to my mom for all her support over the years as without her I would not be where I am today. Thank you, Mom, and I love you.

Second, thanks to my support network back in Alpha Company and my classmates. All of you will eternally be my brothers and sisters, and it's this man's honor to serve with you.

Next, thanks to my friend Jason McDowell. Your advice and input on some of the delicate topics of this book was a big help.

Thanks to the copy editors, Liz Welch and Tiffany Taylor, and to the proofreader Sarah Kaikini at Word One, for all their hard work.

Finally, thanks to Jeff Kellum for your support and assistance in the making of this book.

UMAXISHQMWRVPGBENBZZROIOCMIORMBNYCOOGMZOAAVSLPZOCTQDOZHZROQOHWZKNPRLIDFLZARDOLRTD.

Duty, Service, Honor

About the Author

Sean-Philip Oriyano is the owner of oriyano.com and a veteran of the IT field who has experience in the aerospace, defense, and cybersecurity industries. During his time in the industry, he has consulted and instructed on topics across the IT and cybersecurity fields for small clients up to the enterprise level. Over the course of his career, he has worked with the U.S. military and Canadian armed forces and has taught at locations such as the U.S. Air Force Academy and the U.S. Naval War College.

In addition to his civilian career, Sean is a member of the California State Military Reserve, where he serves as a warrant officer specializing in networking and security. In this role, he works to support the U.S. Army and National Guard on technology issues and training. When not working, he enjoys flying, traveling, skydiving, competing in obstacle races, and cosplaying.

Introduction

If you're preparing to take the CEH exam, you'll undoubtedly want to find as much information as you can about computers, networks, applications, and physical security. The more information you have at your disposal and the more hands-on experience you gain, the better off you'll be when taking the exam. This study guide was written with that goal in mind—to provide enough information to prepare you for the test, but not so much that you'll be overloaded with information that is too far outside the scope of the exam. To make the information more understandable, I've included practical examples and experience that supplements the theory.

This book presents the material at an advanced technical level. An understanding of network concepts and issues, computer hardware and operating systems, and applications will come in handy when you read this book. While every attempt has been made to present the concepts and exercises in an easy-to-understand format, you will need to have experience with IT and networking technology to get the best results.

I've included review questions at the end of each chapter to give you a taste of what it's like to take the exam. If you're already working in the security field, check out these questions first to gauge your level of expertise. You can then use the book to fill in the gaps in your current knowledge. This study guide will help you round out your knowledge base before tackling the exam itself.

If you can answer 85 percent to 90 percent or more of the review questions correctly for a given chapter, you can feel safe moving on to the next chapter. If you're unable to answer that many questions correctly, reread the chapter and try the questions again. Your score should improve.

NOTE

Don't just study the questions and answers! The questions on the actual exam will be different from the practice questions included in this book. The exam is designed to test your knowledge of a concept or objective, so use this book to learn the objectives behind the questions.

Before You Begin Studying

Before you begin preparing for the exam, it's imperative that you understand a few things about the CEH certification. CEH is a certification from the International Council of Electronic Commerce Consultants (EC-Council) granted to those who obtain a passing score on a single exam (number 312-50). The exam is predominantly multiple choice, with some questions including diagrams and sketches that you must analyze to arrive at an answer. This exam requires intermediate to advanced-level experience; you're expected to know a great deal about security from an implementation and theory perspective as well as a practical perspective.

In many books, the glossary is filler added to the back of the text; this book's glossary (located on the companion website at www.sybex.com/go/cehv8) should be considered necessary reading. You're likely to see a question on the exam about what a black or white box test is—not how to specifically implement it in a working environment. Spend your study time learning the various security solutions and identifying potential security vulnerabilities and where they are applicable. Also spend time thinking outside the box about how things work—the exam is also known to alter phrases and terminology—but keep the underlying concept as a way to test your thought process.

The EC-Council is known for presenting concepts in unexpected ways on their exam. The exam tests whether you can apply your knowledge rather than just commit information to memory and repeat it back. Use your analytical skills to visualize the situation and then determine how it works. The questions throughout this book make every attempt to re-create the structure and appearance of the CEH exam questions.

Why Become CEH Certified?

There are a number of reasons for obtaining the CEH certification. These include the following:

Provides Proof of Professional Achievement Specialized certifications are the best way to stand out from the crowd. In this age of technology certifications, you'll find hundreds of thousands of administrators who have successfully completed the Microsoft and Cisco certification tracks. To set yourself apart from the crowd, you need a little bit more. The CEH exam is part of the EC-Council certification track, which includes the other security-centric certifications if you wish to attempt those.

Increases Your Marketability The CEH for several years has provided a valuable benchmark of the skills of a pen tester to potential employers or clients. Once you hold the CEH certification, you'll have the credentials to prove your competency. Moreover, certifications can't be taken from you when you change jobs—you can take that certification with you to any position you accept.

Provides Opportunity for Advancement Individuals who prove themselves to be competent and dedicated are the ones who will most likely be promoted. Becoming certified is a great way to prove your skill level and show your employer that you're committed to improving your skill set. Look around you at those who are certified: They are probably the people who receive good pay raises and promotions.

Fulfills Training Requirements Many companies have set training requirements for their staff so that they stay up to date on the latest technologies. Having a certification program in security provides administrators with another certification path to follow when they have exhausted some of the other industry-standard certifications.

Raises Customer Confidence Many companies, small businesses, and the governments of various countries have long discovered the advantages of being a CEH. Many organizations require that employees and contractors hold the credential in order to engage in certain work activities.

How to Become a CEH Certified Professional

The first place to start on your way to certification is to register for the exam at any Pearson VUE testing center. Exam pricing might vary by country or by EC-Council membership. You can contact Pearson VUE by going to their website (www.vue.com), or in the United States and Canada by calling toll-free 877-551-7587.

When you schedule the exam, you'll receive instructions about appointment and cancellation procedures, ID requirements, and information about the testing center location. In addition, you will be required to provide a special EC-Council–furnished code in order to complete the registration process. Finally, you will also be required to fill out a form describing professional experience and background before a code will be issued for you to register.

NOTE Exam prices and codes may vary based on the country in which the exam is administered. For detailed pricing and exam registration procedures, refer to EC-Council's website at www.eccouncil.org/certification.

After you've successfully passed your CEH exam, the EC-Council will award you with certification. Within four to six weeks of passing the exam, you'll receive your official EC-Council CEH certificate.

Who Should Read This Book?

If you want to acquire a solid amount of information in hacking and pen-testing techniques and your goal is to prepare for the exam by learning how to develop and improve security, this book is for you. You'll find clear explanations of the concepts you need to grasp and plenty of help to achieve the high level of professional competency you need in order to succeed in your chosen field.

If you want to become certified, this book is definitely what you need. However, if you just want to attempt to pass the exam without really understanding security, this study guide isn't for you. You must be committed to learning the theory and concepts in this book to be successful.

NOTE In addition to reading this book, consider downloading and reading the white papers on security that are scattered throughout the Internet.

What Does This Book Cover?

This book covers everything you need to know to pass the CEH exam. Here's a breakdown chapter by chapter:

Chapter 1: Getting Started with Ethical Hacking This chapter covers the purpose of ethical hacking, defines the ethical hacker, and describes how to get started performing security audits.

Chapter 2: System Fundamentals This chapter presents a look at the various components that make up a system and how they are affected by security.

Chapter 3: Cryptography This chapter explores the art and science of cryptography; you'll learn how cryptography works and how it supports security.

Chapter 4: Footprinting and Reconnaissance In this chapter, you'll learn how to gain information from a target using both passive and active methods.

Chapter 5: Scanning Networks This chapter shows you how to gain information about the hosts and devices on a network as well as what the information means.

Chapter 6: Enumeration of Services In this chapter, you'll learn how to probe the various services present on a given host and how to process the information to determine what it means and how to use it for later actions.

Chapter 7: Gaining Access to a System This chapter shows you how to use the information gained from footprinting, scanning, and earlier examinations in order to break into or gain access to a system.

Chapter 8: Trojans, Viruses, Worms, and Covert Channels This chapter covers the varieties of malware and how each can be created, used, or defended against.

Chapter 9: Sniffers This chapter discusses using packet sniffers to gather information that is flowing across the network. You'll learn how to dissect this information for immediate or later use.

Chapter 10: Social Engineering This chapter covers how to manipulate the human being in order to gain sensitive information.

Chapter 11: Denial of Service This chapter includes an analysis of attacks that are designed to temporarily or permanently shut down a target.

Chapter 12: Session Hijacking This chapter covers how to disrupt communications as well as take over legitimate sessions between two parties.

Chapter 13: Web Servers and Web Applications This chapter explains how to break into and examine web servers and applications as well as the various methods of attack.

Chapter 14: SQL Injection In this chapter, you'll learn how to attack databases and data stores using SQL injection to alter, intercept, view, or destroy information.

Chapter 15: Wireless Networking In this chapter, you'll learn how to target, analyze, disrupt, and shut down wireless networks either temporarily or permanently.

Chapter 16: Evading IDSs, Firewalls, and Honeypots This chapter covers how to deal with the common protective measures that a system administrator may put into place; these measures include intrusion detection system (IDSs), firewalls, and honeypots.

Chapter 17: Physical Security The final chapter deals with the process of physical security and how to protect assets from being stolen, lost, or otherwise compromised.

Tips for Taking the CEH Exam

Here are some general tips for taking your exam successfully:

- Bring two forms of ID with you. One must be a photo ID, such as a driver's license. The other can be a major credit card or a passport. Both forms must include a signature.
- Arrive early at the exam center so that you can relax and review your study materials, particularly tables and lists of exam-related information. After you are ready to enter the testing room, you will need to leave everything outside; you won't be able to bring any materials into the testing area.
- Read the questions carefully. Don't be tempted to jump to an early conclusion. Make sure that you know exactly what each question is asking.
- Don't leave any unanswered questions. Unanswered questions are scored against you.
- There will be questions with multiple correct responses. When there is more than one correct answer, a message at the bottom of the screen will prompt you either to "Choose two" or "Choose all that apply." Be sure to read the messages displayed to know how many correct answers you must choose.
- When answering multiple-choice questions about which you're unsure, use a process of elimination to get rid of the obviously incorrect answers first. Doing so will improve your odds if you need to make an educated guess.
- On form-based tests (nonadaptive), because the hard questions will take the most time, save them for last. You can move forward and backward through the exam.
- For the latest pricing on the exams and updates to the registration procedures, visit the EC-Council's website at `www.eccouncil.org/certification`.

What's Included in the Book

I've included several testing features in this book and on the companion website at `www.sybex.com/go/cehv8`. These tools will help you retain vital exam content as well as prepare you to sit for the actual exam:

Assessment Test At the end of this introduction is an assessment test that you can use to check your readiness for the exam. Take this test before you start reading the book; it will help you determine the areas in which you might need to brush up. The answers to the assessment test questions appear on a separate page after the last question of the test. Each answer includes an explanation and a note telling you the chapter in which the material appears.

Objective Map and Opening List of Objectives In the book's front matter, I have included a detailed exam objective map showing you where each of the exam objectives is covered in this book. In addition, each chapter opens with a list of the exam objectives it covers. Use these to see exactly where each of the exam topics is covered.

Exam Essentials Each chapter, just before the summary, includes a number of exam essentials. These are the key topics you should take from the chapter in terms of areas to focus on when preparing for the exam.

Chapter Review Questions To test your knowledge as you progress through the book, there are review questions at the end of each chapter. As you finish each chapter, answer the review questions and then check your answers. The correct answers and explanations are in Appendix A. You can go back to reread the section that deals with each question you got wrong to ensure that you answer correctly the next time you're tested on the material.

Additional Study Tools

I've included a number of additional study tools that can be found on the book's companion website at `www.sybex.com/go/cehv8`. All of the following should be loaded on your computer when you're ready to start studying for the test:

Sybex Test Engine On the book's companion website, you'll get access to the Sybex Test Engine. In addition to taking the assessment test and the chapter review questions via the electronic test engine, you'll find practice exams. Take these practice exams just as if you were taking the actual exam (without any reference material). When you've finished the first exam, move on to the next one to solidify your test-taking skills. If you get more than 90 percent of the answers correct, you're ready to take the certification exam.

Electronic Flashcards You'll find flashcard questions on the website for on-the-go review. These are short questions and answers. Use them for quick and convenient reviewing. There are 100 flashcards on the website.

PDF of Glossary of Terms The glossary of terms is on the companion website in PDF format.

How to Use This Book and Additional Study Tools

If you want a solid foundation for preparing for the CEH exam, this is the book for you. I've spent countless hours putting together this book with the sole intention of helping you prepare for the exam.

This book is loaded with valuable information, and you will get the most out of your study time if you understand how I put the book together. Here's a list that describes how to approach studying:

1. Take the assessment test immediately following this introduction. It's okay if you don't know any of the answers—that's what this book is for. Carefully read over the explanations for any question you get wrong, and make a note of the chapters where that material is covered.
2. Study each chapter carefully, making sure that you fully understand the information and the exam objectives listed at the beginning of each one. Again, pay extra-close attention to any chapter that includes material covered in the questions that you missed on the assessment test.
3. Read over the summary and exam essentials. These highlight the sections from the chapter with which you need to be familiar before sitting for the exam.

4. Answer all of the review questions at the end of each chapter. Specifically note any questions that confuse you, and study those sections of the book again. Don't just skim these questions—make sure you understand each answer completely.
5. Go over the electronic flashcards. These help you prepare for the latest CEH exam, and they're great study tools.
6. Take the practice exams.

Exam 312-50 Exam Objectives

The EC-Council goes to great lengths to ensure that its certification programs accurately reflect the security industry's best practices. They do this by continually updating their questions with help from subject matter experts (SMEs). These individuals use their industry experience and knowledge together with the EC-Council's guidance to create questions that challenge a candidate's knowledge and thought processes.

Finally, the EC-Council conducts a survey to ensure that the objectives and weightings truly reflect job requirements. Only then can the SMEs go to work writing the hundreds of questions needed for the exam. Even so, they have to go back to the drawing board for further refinements in many cases before the exam is ready to go live in its final state. Rest assured that the content you're about to learn will serve you long after you take the exam.

NOTE

Exam objectives are subject to change at any time without prior notice and at the EC-Council's sole discretion. Visit the certification page of the EC-Council's website at `www.eccouncil.org` for the most current listing of exam objectives.

The EC-Council also publishes relative weightings for each of the exam's objectives. The following table lists the five CEH objective domains and the extent to which they are represented on the exam. As you use this study guide, you'll find that we have administered just the right dosage of objective knowledge by tailoring coverage to mirror the percentages that the EC-Council uses.

Domain	% of exam
Analysis/Assessment	16%
Security	26%
Tools/Systems/Programs	32%
Procedures/Methodology	20%
Regulation/Policy	4%

Objectives

Objective	Chapter
Background	
Networking technologies (e.g., hardware, infrastructure)	2
Web technologies (e.g., Web 2.0, Skype)	13
Systems technologies	2
Communication protocols	2, 9
Malware operations	11
Mobile technologies (e.g., smartphones)	10
Telecommunication technologies	2
Backups and archiving (e.g., local, network)	2
Analysis/Assessment	
Data analysis	9, 14
Systems analysis	4, 5, 6
Risk assessments	1
Technical assessment methods	1
Security	
Systems security controls	2
Application/fileserver	2
Firewalls	2
Cryptography	3
Network security	2
Physical security	17
Threat modeling	17
Verification procedures (e.g., false positive/negative validation)	16
Social engineering (human factors manipulation)	10
Vulnerability scanners	5
Security policy implications	1, 17
Privacy/confidentiality (with regard to engagement)	1
Biometrics	4
Wireless access technology (e.g., networking, RFID, Bluetooth)	9, 15
Trusted networks	2
Vulnerabilities	2, 5, 7, 12, 13, 14
Tools/Systems/Programs	
Network/host-based intrusion	16

Network/wireless sniffers (e.g., Wireshark, Airsnort)	9
Access control mechanisms (e.g., smart cards)	3
Cryptography techniques (e.g., IPSec, SSL, PGP)	3
Programming languages (e.g., C++, Java, C#, C)	13
Scripting languages (e.g., PHP, JavaScript)	13, 14
Boundary protection appliances (e.g., DMZ)	2, 16
Network topologies	2
Subnetting	2
Port scanning (e.g., NMAP)	5
Domain name system (DNS)	2, 12
Routers/modems/switches	2
Vulnerability scanner (e.g., Nessus, Retina)	5
Vulnerability management and protection systems (e.g., Foundstone, Ecora)	5
Operating environments (e.g., Linux, Windows, Mac)	2, 7
Antivirus systems and programs	8
Log analysis tools	16
Security models	17
Exploitation tools	11
Database structures	14
Procedures/Methodology	
Cryptography	3
Public key infrastructure (PKI)	3
Security Architecture (SA)	17
Service-Oriented Architecture (SOA)	14
Information security incident management	17
N-tier application design	14
TCP/IP networking (e.g., network routing)	2, 12
Security testing methodology	1
Regulation/Policy	
Security policies	17
Compliance regulations (e.g., PCI)	17
Ethics	
Professional code of conduct	1
Appropriateness of hacking activities	1

Assessment Test

1. What is the focus of a security audit or vulnerability assessment?
   - **A.** Locating vulnerabilities
   - **B.** Locating threats
   - **C.** Enacting threats
   - **D.** Exploiting vulnerabilities

2. What kind of physical access device restricts access to a single individual at any one time?
   - **A.** Checkpoint
   - **B.** Perimeter security
   - **C.** Security zones
   - **D.** Mantrap

3. Which of the following is a mechanism for managing digital certificates through a system of trust?
   - **A.** PKI
   - **B.** PKCS
   - **C.** ISA
   - **D.** SSL

4. Which protocol is used to create a secure environment in a wireless network?
   - **A.** WAP
   - **B.** WPA
   - **C.** WTLS
   - **D.** WML

5. What type of exercise is conducted with full knowledge of the target environment?
   - **A.** White box
   - **B.** Gray box
   - **C.** Black box
   - **D.** Glass box

6. You want to establish a network connection between two LANs using the Internet. Which technology would best accomplish that for you?
   - **A.** IPSec
   - **B.** L2TP