CISSP® Study Guide

CISSP® Study Guide

Eric Conrad

Seth Misenar

Joshua Feldman

Technical Editor

Kevin Riggins

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

Acquiring Editor: Rachel Roumeliotis
Development Editor: Matthew Cater
Project Manager: Andre Cuello
Designer: Alisa Andreola

Syngress is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Conrad, Eric, 1967–
CISSP study guide / Eric Conrad, Seth Misenar, Joshua Feldman.
p. cm.
ISBN 978-1-59749-563-9
1. Electronic data processing personnel—Certification. 2. Computer networks—Examinations—Study guides. I. Misenar, Seth. II. Feldman, Joshua. III. Title.
QA76.3.C497 2010
004.6—dc22 2010018643

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN: 978-1-59749-563-9

Printed in the United States of America
10 11 12 13 14 10 9 8 7 6 5 4 3 2 1

For information on all Syngress publications visit our website at www.syngress.com

Contents

Acknowledgments

I need to first thank my wife Melissa and my children Eric and Emma, for their love and patience while I wrote this book. Thank you to contributing authors and my friends Joshua Feldman and Seth Misenar.

Thank you to my teachers and mentors: thank you Miss Gilmore, for sending me on my way. Thank you Dave Curado and Beef Mazzola, for showing me the right way to do it. Thank you Stephen Northcutt, Alan Paller, Deb Jorgensen, Scott Weil, Eric Cole, Ed Skoudis, Johannes Ullrich, and many others from the SANS Institute, for showing me how to take it to the next level.

I would like to thank the supergroup of information security professionals who answered my last minute call, and collectively wrote the 500 questions comprising the two sets of online practice exams: Rodney Caudle, David Crafts, Bruce Diamond, Jason Fowler, Philip Keibler, Warren Mack, Eric Mattingly, Ron Reidy, Mike Saurbaugh, and Gary Whitsett.

Thank you to Michael Strickland for help with figures in Chapter 3. Thank you Rachel Roumeliotis and Matthew Cater of Syngress, for the support and dedication to this book.

Contributing author Seth Misenar writes the following: "I would like to thank my wife, Rachel, the love of my life, who showed continued patience, support, and strength when entertaining two young children throughout this writing process. I am grateful to my children, Jude and Hazel, who, at 3 and 0, were amazingly gracious when daddy had to write. And I count myself lucky to have such wonderful parents, Bob and Jeanine, who, as always, provided much of their time to ensure that my family was taken care of during this writing period."

About the authors

LEAD AUTHOR

Eric Conrad (CISSP®, GIAC GSE, GPEN, GCIH, GCIA, GCFA, GAWN, GSEC and Security+) is a SANS Certified Instructor and is a partner with Backshore Communications, which provides information warfare, penetration testing, incident handling, and intrusion detection consulting services. Eric started his professional career in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care, in roles ranging from systems programmer to security engineer to HIPAA security officer and ISSO. He has taught over 1000 students in courses including SANS Management 414: CISSP®, Security 560: Network Penetration Testing and Ethical Hacking, Security 504 Hacker Techniques, Exploits & Incident Handling, and others.

Eric is a graduate of the SANS Technology Institute with a Master of Science degree in Information Security Engineering. Eric currently lives in Peaks Island, Maine with his family, Melissa, Eric and Emma.

CONTRIBUTING AUTHORS

Seth Misenar (CISSP®, GPEN, GCIH, GCIA, GCFA, GWAPT, GCWN, GSEC, MCSE, MCDBA) is a Certified Instructor with the SANS Institute and also serves as lead consultant for Jackson, Mississippi-based Context Security. Seth's background includes security research, network and Web application penetration testing, vulnerability assessment, regulatory compliance efforts, security architecture design, and general security consulting. He has previously served as a physical and network security consultant for Fortune 100 companies as well as the HIPAA and information security officer for a state government agency. Seth teaches a variety of courses for the SANS Institute, including Security Essentials, Web Application Penetration Testing, Hacker Techniques, and the CISSP® course.

Seth is pursuing a Master of Science degree in Information Security Engineering from the SANS Technology Institute and holds a Bachelor of Science degree from Millsaps College. Seth resides in Jackson, Mississippi with his family, Rachel, Jude, and Hazel.

Joshua Feldman (CISSP®, NSA IAM) has supported the Department of Defense Information Systems Agency as a contractor working for SAIC, Inc. Since 2002, he was a subject matter expert and training developer for DISA's cyber security mission. During his tenure, he contributed to the DoD 8500 series, specifically conducting research and authoring sections of the DoD 8570.01-M, also known as the DoD IA Workforce Improvement Program. He has taught well over 1000 DoD students through his "DoD IA Boot Camp" course. He is also a subject matter expert for the Web-based Information Assurance awareness training that every DoD user is required to take each year as part of their security awareness curriculum. He is a regular presenter and panel member at the Information Assurance Symposium, hosted by both DISA and NSA.

Before joining the support team at DoD/DISA, Joshua spent time as an IT Sec engineer working for the Department of State, Diplomatic Security. There, he travelled to embassies worldwide to conduct Tiger Team assessments of the security of each embassy. Joshua got his start in the IT Security field when he left his position teaching science for Montgomery County Public Schools, Maryland and went to work for NFR Security Software. At the time, NFR was one of the leading companies producing Network Intrusion Detection systems.

ABOUT THE TECHNICAL EDITOR

Kevin Riggins (CISSP®) has over 22 years of experience in Information Technology and has focused on Information Security since 1999. He has been a Certified Information Systems Security Professional since 2004 and currently works for a Fortune 500 financial service company where he leads a team of information security analysts responsible for internal consulting, risk assessments, and vendor security reviews. He writes about various information security topics on his blog, Infosec Ramblings (http://www.infosecramblings.com), his articles have been published in (IN)Secure magazine, and he is a frequent speaker at conference and industry association meetings.