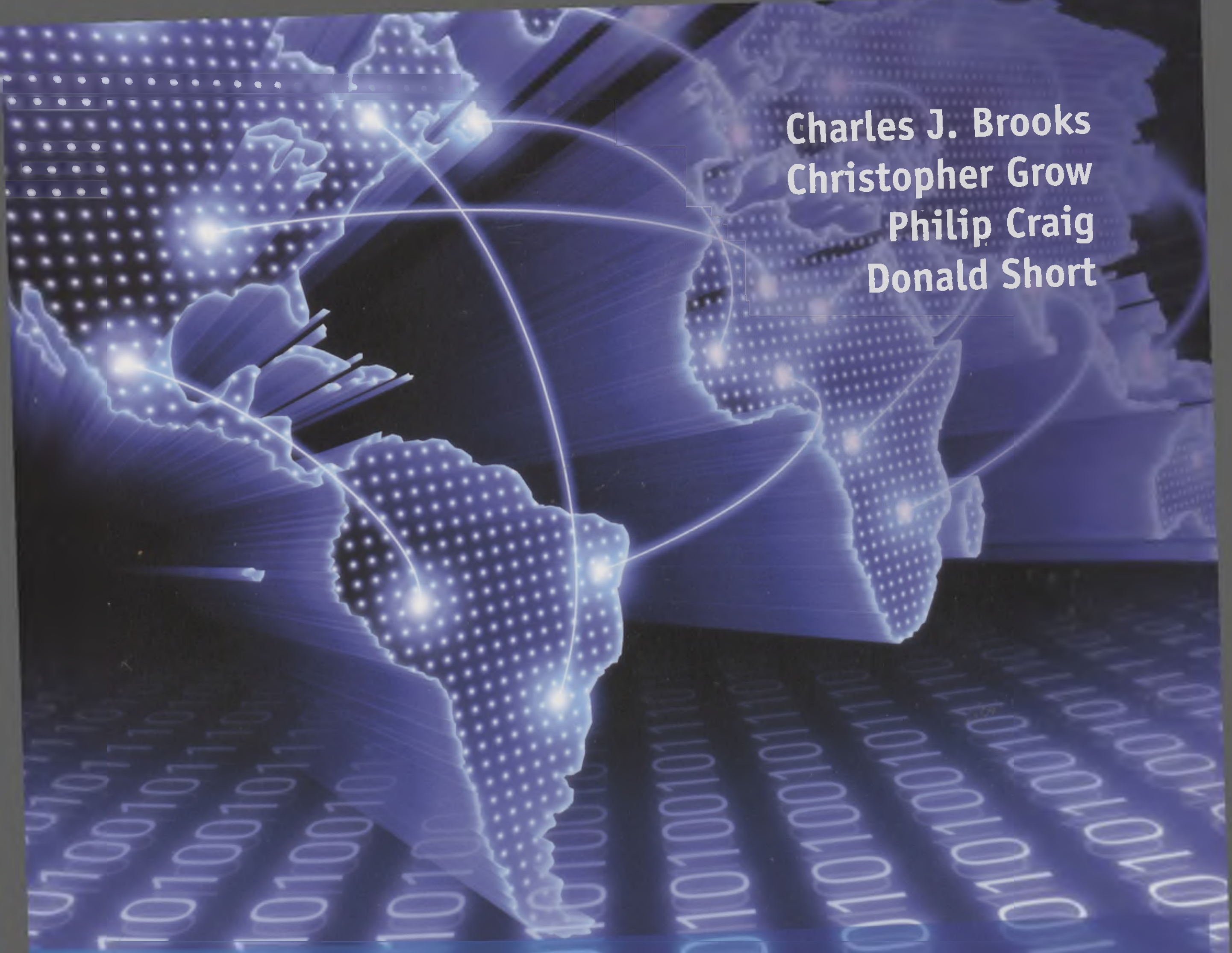


Charles J. Brooks
Christopher Grow
Philip Craig
Donald Short

Cybersecurity

ESSENTIALS

SYBEX
A Wiley Brand

CYBERSECURITY

ESSENTIALS

Charles J. Brooks
Christopher Grow
Philip Craig
Donald Short

SYBEX®
A Wiley Brand

Development Editor: David Clark
Technical Editors: Raymond Blockmon, Chris Culling, Jeff Parker
Production Editor: Athiyappan Lalith Kumar
Copy Editor: Kathy Carlyle
Editorial Manager: Mary Beth Wakefield
Production Manager: Kathleen Wisor
Executive Editor: Jim Minatel
Proofreader: Nancy Bell
Indexer: Johnna VanHoose Dinse
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: © ktsdesign/Shutterstock

Published simultaneously in Canada
ISBN: 978-1-119-36239-5
ISBN: 978-1-119-36243-2 (ebk)
ISBN: 978-1-119-36245-6 (ebk)
Manufactured in the United States of America

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: 2018943782

C10003887_082218

To my wife Robbie, for all of her understanding, support, and help with these projects, as well as Robert, Jamaica, Michael, and Joshua.
Charles Brooks

To my close friends and family here and gone who have stood by me and encouraged me along my way. Your support through the years, mental, emotional, and financial, has brought me to this point. I dedicate this work to all of you, without which this would not have been possible for me.
Christopher Grow

To my wife Caralee, who has endured many times over the years my travels, my long stays in our nation's capital, and mostly her understanding of the importance of my commitment to cybersecurity. As we celebrate her birthday on September 11 every year, we are reminded of what it means to our daily lives.
Philip Craig

To my family whose grace and support have amazed me for decades. My loving wife of 33 years, Norma, and my children Kenny and Breanne continue to support my efforts and endure the challenges of my entrepreneurial life.
Donald Short

Acknowledgments

As always, I want to thank the staff at ETG/Marcraft for making it easy to turn out a good product. In particular, thanks to Cathy Boulay and Luke Johns from the Product Development department for their excellent work in getting the text and graphics ready to go and looking good.

Many thanks as well to Jeff Riley, whom I've known and worked with in the book production business for many years. Thanks for putting together another great project.

—Charles Brooks

I would like to start by thanking some of the many people who have made what has become my repository of knowledge and skill available to help make this book possible. First there is my father David P. Grow. His knowledge, mentoring, patience, and understanding started my journey down the career path of computer support and computer networking.

I would also like to thank all of my mentors along the way who have increased my skills and knowledge. Whether they were employers or colleagues, each mentor has made contributions to my knowledge and skill that helped make this all possible. Especially the support staff and leadership here with my current employer at ETG/Marcraft: Charles Brooks, Kevin Smith, Cathy Boulay, Grant Ter-Oganov and any personnel working behind the scenes that I did not meet.

Lastly I would like to thank my close friends and family for all their help and support as I worked through the process of creating my contribution to this book.

—Christopher Grow

To the folks who commit their lives and careers developing new approaches to cybersecurity that protects the immense landscape of computing infrastructures from acts of malicious and sometimes deadly outcomes of cyber attacks, I dedicate these works to you. The next generation of cyber-protectors will gain significant value from this book and hopefully will find its content sparking new dedication to the cyber challenges we will face in the years ahead.

To the leadership at ETG/Marcraft whose vision recognizes the value of the teaching through hands-on experiences and not just the texts, thank you for recognizing and implementing your approach to our trade.

—Philip Craig

I would like to thank my customers and associates from the past 25 plus years who have helped me grow and learn at a rate I would not have thought possible.

—Donald Short

About the Authors

Charles J. Brooks is currently co-owner and vice president of Educational Technologies Group Inc., as well as co-owner of eITPrep LLP, an online training company. He is in charge of research and product development at both organizations.

A former electronics instructor and technical writer with the National Education Corporation, Charles taught and wrote on post-secondary ETG curriculum, including introductory electronics, transistor theory, linear integrated circuits, basic digital theory, industrial electronics, microprocessors, and computer peripherals.

Charles has authored several books, including seven editions of *A+ Certification Training Guide, The Complete Introductory Computer Course,* and *IBM PC Peripheral Troubleshooting and Repair.* He also writes about green technologies, networking, residential technology integration, and IT convergence.

Christopher M. Grow is currently the Technical Services Manager for Educational Technologies Group. He is responsible for product support, solution development, onsite implementation/installation, and instructor support and training for a wealth of cybersecurity and information technology products. He also is involved in program management and contributes in R&D of new products and revisions of current offerings.

Christopher has been a consultant and contractor in the IT industry for over 20 years. As an Information Security and Surveillance manager for a casino in Washington State, Christopher helped design and implement security policies, frameworks, and training to protect and segregate public and private information for the casino and their customers. He also helped to design procedures and train personnel on the physical security aspects of the casino industry.

Philip Craig is the founder of BlackByte Cyber Security, LLC, a consultancy supporting the Pacific Northwest National Laboratory (PNNL) research and national security agendas as well as the National Rural Electric Cooperative Association and National Rural Telecommunications Cooperative.

For many years, Phil served as a Senior Cyber Security Research Scientist at PNNL, where he provided engineering and program management support in the fields of cybersecurity, supervisory control and data acquisition (SCADA) technologies, computing, and communications infrastructure.

This included development of complex system and policy solutions in a variety of critical infrastructures including the nuclear power, electric power, and water sectors. He developed and deployed both strategic and tactical cybersecurity defensive solutions for the electric power and nuclear sectors.

Donald Short is the President of One World Telecommunications, Inc., an Internet Service Provider in Kennewick, Washington, where he both manages the business and programs web and database applications.

Don has been both a pharmacist and computer scientist for over 35 years, working in many programming languages on a variety of network architectures, and has developed large and complex online content and learning management systems.

Contents

PART IV SECURING THE PERIMETER 449

Chapter 18 Perimeter Security in the Real World 451

Chapter 19 Understanding the Environment 457

Chapter 20 Hiding the Private Network 487

CHAPTER 23 Tools and Utilities 565

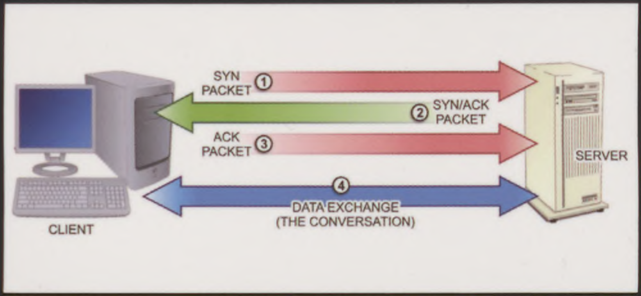
CHAPTER 24 Identifying and Defending Against Vulnerabilities 591

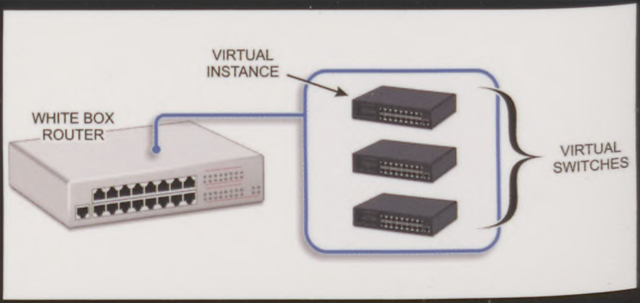
An easy-to-use and comprehensive introduction to cybersecurity

Cybersecurity Essentials provides a comprehensive introduc
cybersecurity certifications. It covers the four distinct cha a-
structure, securing devices, securing local networks, and s e
the fundamental concepts of each challenge and include re y
computing. The text offers a summary of the key concepts, review questions, and hands-on exerc an
understanding of key concepts.

Learn these fundamentals of security infrastructure—and more:

- Basic security and surveillance systems
- Intrusion detection and reporting systems
- Local host security
- Securing devices
- Protecting the inner peri
- Protecting remote access
- Local network Security
- Network topologies and protocols





This *Essentials* book features:

- Chapter-opening learning objectives
- Essentials and Beyond—summaries and additional suggested exercises
- Hands-on exercises

About the Authors

Charles J. Brooks is co-owner and vice president of Educational Technologies Group Inc., as well as co-owner of eITPrep LLP, an online training company. **Christopher Grow** is the president of A.C.C.N.S. Consulting and the Technichal Services manager for Educational Technologies Group L.L.C. with 20+ years of IT/IS and cyber security experience. **Philip Craig** is the founder of BlackByte Cyber Security, LLC, a consultancy supporting the Pacific Northwest National Laboratory (PNNL) research and national security agendas. **Donald Short** is the President of One World Telecommunications, Inc., an Internet Service Provider in Kennewick.

www.sybex.com

$ 40.00 USA / £ 32.99 UK

Cover Design: Wiley
Cover Image: © ktsdesign/Shutterstock

ISBN 978-1-119-36239-5
54000
9 781119 362395

Also available as an e-book

SYBEX
A Wiley Brand

COMPUTERS / Security