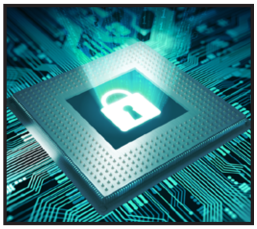
Thomas J. Mowbray

Cybersecurity

Managing Systems, Conducting Testing, and Investigating Intrusions

WILEY



Cybersecurity

Managing Systems, Conducting Testing, and Investigating Intrusions

Thomas J. Mowbray, PhD,
CEA^2, CPHIMS, GPEN Gold

WILEY

Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published by John Wiley & Sons, Inc., Indianapolis, Indiana
Published simultaneously in Canada

ISBN: 978-1-118-69711-5
ISBN: 978-1-118-69704-7 (ebk)
ISBN: 978-1-118-84965-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

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 website may provide or recommendations it may make. Further, readers should be aware that Internet websites 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 please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States 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: 2013948021

Dedicated to my lovely wife, Kate Mowbray, CPA

About the Author

Thomas J. Mowbray, PhD, SANS GPEN Gold is the Chief Enterprise Architect of The Ohio State University. In addition, he is a

- Zachman Certified Enterprise Architect
- FEAC Institute Certified Enterprise Architect
- HIMSS Certified Professional in Healthcare Information Management Systems
- Former Network Penetration Tester, Cyber Toolsmith & Cyber Lab Manager
- Founder of the Northrup Grumman / TASC Cyber Warfare Community of Interest
- SANS Certified Network Penetration Tester (GPEN) with vetted Gold Paper Research

He has coauthored two books: *AntiPatterns: Refactoring Software, Architectures, and Projects in Crisis* (1998 John Wiley & Sons, ISBN 978-047-1-19713-3) and *Software Architect Bootcamp* (2003 Prentice Hall, ISBN 978-0-13-141227-9). He is also the Associate Editor of the *Journal of Enterprise Architecture*. You can connect with Dr. Mowbray on LinkedIn.

About the Technical Editor

Rob Shimonski is a highly experienced technologist and business leader with more than 20 years of real-world experience in the field. Rob started his professional career in the military and is now focused primarily on healthcare. Rob has worked for countless companies, including Microsoft, Cisco, and the National Security Agency. As a security expert, Rob has been entrenched in the cyber-world for two decades and has lived through the technical evolution of the “war.” Rob is also a best-selling author and editor with more than 15 years’ experience developing, producing, and distributing print media in the form of books, magazines, and periodicals. To date, Rob has successfully helped create more than 100 books that are currently in circulation.

Credits

Executive Editor
Carol Long

Project Editor
Charlotte Kughen

Technical Editor
Rob Shimonski

Senior Production Editor
Kathleen Wisor

Copy Editor
Faunette Johnson

Editorial Manager
Mary Beth Wakefield

Freelancer Editorial Manager
Rosemarie Graham

Associate Director of Marketing
David Mayhew

Marketing Manager
Ashley Zurcher

Business Manager
Amy Knies

Vice President and Executive Group Publisher
Richard Swadley

Associate Publisher
Jim Minatel

Project Coordinator, Cover
Katie Crocker

Compositor
Cody Gates,
Happenstance Type-O-Rama

Proofreader
Nancy Carrasco

Indexer
Robert Swanson

Cover Image
©iStockphoto.com/Henrik5000

Cover Designer
Ryan Sneed

Acknowledgments

Thanks to the SANS Institute, in particular Allan Paller and Ed Skoudis, for conducting terrific cybersecurity training programs. Thanks also to the NGC/TASC Corporation for sponsoring SANS training, the TASC Institute security training programs, and for encouraging me to found the NGC/TASC Cyber Warfare Community of Interest.

Special thanks to my SANS gold paper advisor, Dr. Kees Leune, who contributed many ideas and much encouragement to Chapter 14, which was originally published as a SANS Gold Paper. I am very fortunate to have someone with his credentials, including a recent PhD in Information Security, advising on Chapter 14.

Many thanks are also due to Wellhouse Consultants for their free online Python tutorial on multithreading (`www.wellho.net/`). The threaded code in Chapters 6 and 14 is original, but it is inspired by their tutorial example, in which they also claim dramatic speed-up over serial processing.

Gail Tyron, IBM, supplied many cloud computing practice examples included in Chapter 12. Ms. Tyron is an IT security policy subject matter expert, specializing the NIST 800 series, with visibility into cloud practices across many enterprises. Thanks to Mr. Roger Caslow who continues to encourage this project.

Generous thanks to my editorial team at John Wiley & Sons. They saw the vision of this project and stuck with me all the way to the goal!

Contents at a Glance

Contents

Introduction

This book will teach you the concepts, skills, and tools you need to survive and thrive in today's threat-ridden and target-rich cyber environment.

Who This Book Is For

The book is written for several core audiences:

- Cybersecurity graduate and undergraduate students learning core curriculum in network security
- Cybersecurity practitioners expanding their expertise in deep skills such as advanced log analysis and network programming
- Enterprise architects and information technology (IT) professionals who seek to deepen their practical knowledge of cybersecurity

What This Book Covers

Instead of the usual textbook formalities, this book focuses on practical, useful real-world skills for the protection of networks, systems, and data against innovative cyber threats.

This book is written to provide practical, advanced, undergraduate-level network security expertise. U.S. requirements for this level of expertise are clearly articulated by academic and industry members of CyberWatchCenter.org, one of the organizations in charge of the U.S. Comprehensive National Cyber Security

Initiative (CNCI) #8 on cybersecurity education. The table of contents in this book derives from the consensus of the cyber industry and two- and four-year college cyber faculty.

How This Book Is Structured

This book is organized in parts:

- Part I: Cyber Network Security Concepts
- Part II: Cyber Network Security Hands-On
- Part III: Cyber Network Application Domains

Part I is a conceptual discourse. From the executive perspective, Chapter 1 introduces you to the cybersecurity domain and some of its key challenges—in particular, educating a new generation of hands-on cybersecurity professionals.

From the business management perspective, Chapter 2 uses antipatterns to explain the most common mistakes and bad habits in computer security today. Antipatterns are fun to read and discuss because they highlight some of the most ridiculous and naive things people do that result in significant security gaps. If you avoid the worst antipatterns, your situation will dramatically improve. This is especially true of cybersecurity. The choice of cyber antipatterns in the chapter is derived from an assessment of the most critical cyber antipatterns in current organizations, networks, and systems.

Chapter 3 introduces the Zachman Framework and articulates a vision for resolving cybersecurity issues by transforming enterprises. Enterprises that have self-knowledge (that is, enterprise architecture) are able to change and respond with agility to cybersecurity challenges. Future organizations must adopt this vision for competitive business reasons as well as cybersecurity reasons.

Part II is almost entirely a hands-on tutorial for cybersecurity techniques, including assignments using cyber labs from Syracuse University's SEED: A Suite of Instructional Laboratories for Computer Security Education. The material in the chapters progresses from a more basic to a very advanced hands-on introduction to enterprise network security. I review networking essentials, cover practical skills in network administration, review network security programming, and then explain network penetration, Google hacks, BackTrack customization, vulnerability testing, and the certification testing process. The final chapter in this part is a real-world introduction to network defense, explaining the scripts and procedures for conducting network investigations and advanced log analysis.

Part III covers several important security application domains, such as small businesses, data centers, clouds, and healthcare IT.

Throughout the book are hands-on exercises with online software resources called SEED Labs: Developing Instructional Laboratories for Computer Security Education. These are the invention of Professor Kevin Du from Syracuse University, who had the great foresight to create hands-on coursework independent of any single textbook. An instructor manual is available from Professor Du containing exemplary exercise solutions. In addition, you can find instructor ancillaries available online for this book, including a course syllabus, a test bank, and PowerPoint slides for each chapter.

In profound ways, this is day zero in cybersecurity. The entire regime of paper-driven compliance, policy-driven certifications, and signature-based defenses has failed miserably (i.e., indicative of antipatterns). This book offers practical ways to approach cyber defenses, which leverage ongoing innovations in intrusion detection/prevention and malware defense. My vision is that this book sets a new level of expectations for advanced undergraduate education in network security and plays a role in turning the tide against cyber criminals and cyber warriors attacking our society.

How This Book Came About

I was a successful enterprise architect, but always wanted to add cybersecurity to my bag of tricks. I decided to make a radical career change by transitioning to hands-on cybersecurity testing. I earned a SANS Institute GPEN certification (and then GPEN Gold) performing security research which allowed me, with encouragement from the SANS Institute's Alan Paller, to jump right over the heads of a lot of CISSPs into several exciting security roles. I enthusiastically took on rudimentary tasks such as software installation, virtual machine migration, and administering networks, as well as, advanced tasks such as security toolkit customization and hands-on IT security certification testing. What I discovered was an eye opener.

I wrote up everything useful that I learned and added even more content to complete a body of knowledge, with a specific purpose in mind: resolving the U.S. crisis in cybersecurity by providing an essential, but missing, educational tool. People with the skills contained in this book can be valuable members of any cybersecurity team, from the most rudimentary and useful skills to some of the most advanced.

What You Need to Use This Book

To run the Linux-based tools and scripts, download a recent release of BackTrack Linux from `http://www.backtrack-linux.org/`. Current releases of Windows should be able to run the Windows Command Line scripts and commands in Chapters 4 and 6.

The source code for the samples is available for download from the Wrox website at:

```
www.wiley.com/go/cybersecurity
```

Conventions

To help you get the most from the text and keep track of what's happening, we've used a number of conventions throughout the book.

WARNING Warnings hold important, not-to-be-forgotten information that is directly relevant to the surrounding text.

NOTE Notes indicates notes, tips, hints, tricks, or and asides to the current discussion.

As for styles in the text:

- I *highlight* new terms and important words when I introduce them.
- I show keyboard strokes like this: Ctrl+A.
- I show file names, URLs, and code within the text like so: `persistence.properties`.
- I present code as shown here:

```
I use a monofont type with no highlighting for most code examples.
```

Source Code

As you work through the examples in this book, you may choose either to type in all the code manually, or to use the source code files that accompany the book. The source code from Chapter 9 is available for download at `www.wrox.com`. Specifically for this book, the code download is on the Download Code tab at:

```
www.wiley.com/go/cybersecurity
```

You can also search for the book at `www.wrox.com` by ISBN (the ISBN for this book is 978-1-118-69711-5) to find the code. And a complete list of code downloads for all current Wrox books is available at `www.wrox.com/dynamic/books/download.aspx`.

Most of the code on www.wrox.com is compressed in a .ZIP, .RAR archive, or similar archive format appropriate to the platform. Once you download the code, just decompress it with an appropriate compression tool.

Ancillary Files

To aide college professors and other instructors who are using this book to teach, the author has created ancillary supplements, in particular a sample course syllabus, a chapter-by-chapter test bank, and chapter-by-chapter PowerPoint slide decks. These materials are available at

```
www.wiley.com/go/cybersecurity
```

You will also find exercise assignments at the end of each chapter, and online hands-on laboratory exercises from the Syracuse University SEED Labs embedded throughout the book.

Errata

We make every effort to ensure that there are no errors in the text or in the code. However, no one is perfect, and mistakes do occur. If you find an error in one of our books, like a spelling mistake or faulty piece of code, we would be very grateful for your feedback. By sending in errata, you may save another reader hours of frustration, and at the same time, you will be helping us provide even higher quality information.

To find the errata page for this book, go to

```
www.wiley.com/go/cybersecurity
```

And click the Errata link. On this page you can view all errata that has been submitted for this book and posted by Wrox editors.

If you don't spot "your" error on the Book Errata page, go to www.wrox.com/contact/techsupport.shtml and complete the form there to send us the error you have found. We'll check the information and, if appropriate, post a message to the book's errata page and fix the problem in subsequent editions of the book.

P2P.WROX.COM

For author and peer discussion, join the P2P forums at `http://p2p.wrox.com`. The forums are a Web-based system for you to post messages relating to Wrox books and related technologies and interact with other readers and technology users. The forums offer a subscription feature to e-mail you topics of interest of your choosing when new posts are made to the forums. Wrox authors, editors, other industry experts, and your fellow readers are present on these forums.

At `http://p2p.wrox.com`, you will find a number of different forums that will help you, not only as you read this book, but also as you develop your own applications. To join the forums, just follow these steps:

1. Go to `http://p2p.wrox.com` and click the Register link.
2. Read the terms of use and click Agree.
3. Complete the required information to join, as well as any optional information you wish to provide, and click Submit.
4. You will receive an e-mail with information describing how to verify your account and complete the joining process.

NOTE You can read messages in the forums without joining P2P, but in order to post your own messages, you must join.

After you join, you can post new messages and respond to messages other users post. You can read messages at any time on the web. If you would like to have new messages from a particular forum e-mailed to you, click the Subscribe to this Forum icon by the forum name in the forum listing.

For more information about how to use the Wrox P2P, be sure to read the P2P FAQs for answers to questions about how the forum software works, as well as many common questions specific to P2P and Wrox books. To read the FAQs, click the FAQ link on any P2P page.

Part

I

Cyber Network Security Concepts

In This Part

CHAPTER

1

Executive Summary

Effective cybersecurity is a critical capability for the defense and preservation of civil society. Cyber crime is one of the world's largest and fastest-growing categories of crime. Cyber criminals are responsible for more than $1 trillion USD in stolen funds and other assets, with crime in some segments growing 300 percent per year. Cyber espionage is epidemic and pervasive; even the world's smartest companies and government institutions have terabytes of intellectual property and financial assets being lost annually via the Internet. Concealed malicious actors even threaten our electrical power grids, global financial systems, air traffic control systems, telecommunications systems, healthcare systems, and nuclear power plants.

Chances are good that your current organization is being attacked right now: cyber criminals, civilian/military cyber warriors, and global competitors are deeply entrenched in your network. If you have information worth stealing, it is likely that the attackers are on your internal network, exfiltrating data from your end users, and controlling key administrative nodes. If organizations don't change the way they are defending themselves, personal identifying information, bank account and credit card numbers, and intellectual property that defines competitive advantage will continue to be stolen.

The threat is to all civil society. If cyber attackers scrambled all the data on Wall Street and Bond Street, wiping out all investments and retirement accounts based in the U.S. and U.K., the consequences are unthinkable. (And this scenario is a real possibility.) The goal of this book is to lay the foundation for solving this critical problem in earnest.

U.S. government policy experts are quite concerned about the strategic gap in cyber skills, claiming that in 2008 the U.S. had only 1,000 world-class cyber experts but would require 20,000 to 30,000 to adequately handle cyberspace offense and defense. I believe that estimate is quite low. There are 25,000,000 business establishments that need cyber defenses in the U.S. alone, according to the census bureau. Certainly, hundreds of thousands of technologists with the kinds of skills and education presented in this book will be needed to fully defend civil society.

Why Start with Antipatterns?

To successfully make a change, the first step is to admit you have a problem. The civilized world is in a dire predicament regarding cyber threats. Solving cybersecurity issues requires radical new ways of thinking, and, paradoxically, a return to first principles and common sense—in other words, ruthless pragmatism.

Antipatterns employ psychological frameworks for solving problems whose causes involve habitual mistakes. Antipatterns require a mind shift from the dispassionate mindsets of mathematics and engineering into the judgmental milieu of enterprise architecture and organizational change.

NOTE Some people have criticized antipatterns as being anti-intellectual. Antipatterns are a way of thinking clearly about habitual causes, serious problems, and effective solutions.

Antipatterns have been summarized by the quip, "Technology is not the problem…people are the problem." But, changing people's minds is very difficult. So, you need powerful psychology to do that.

NOTE The classic paradigm of organizational change is: You send your people out on a rickety bridge toward a pot of gold and then start a fire behind them so they can never go back to old ways.

Antipatterns have ancient roots in governance, law enforcement, religion, and public administration. In a perverse sense, antipatterns are an adult form