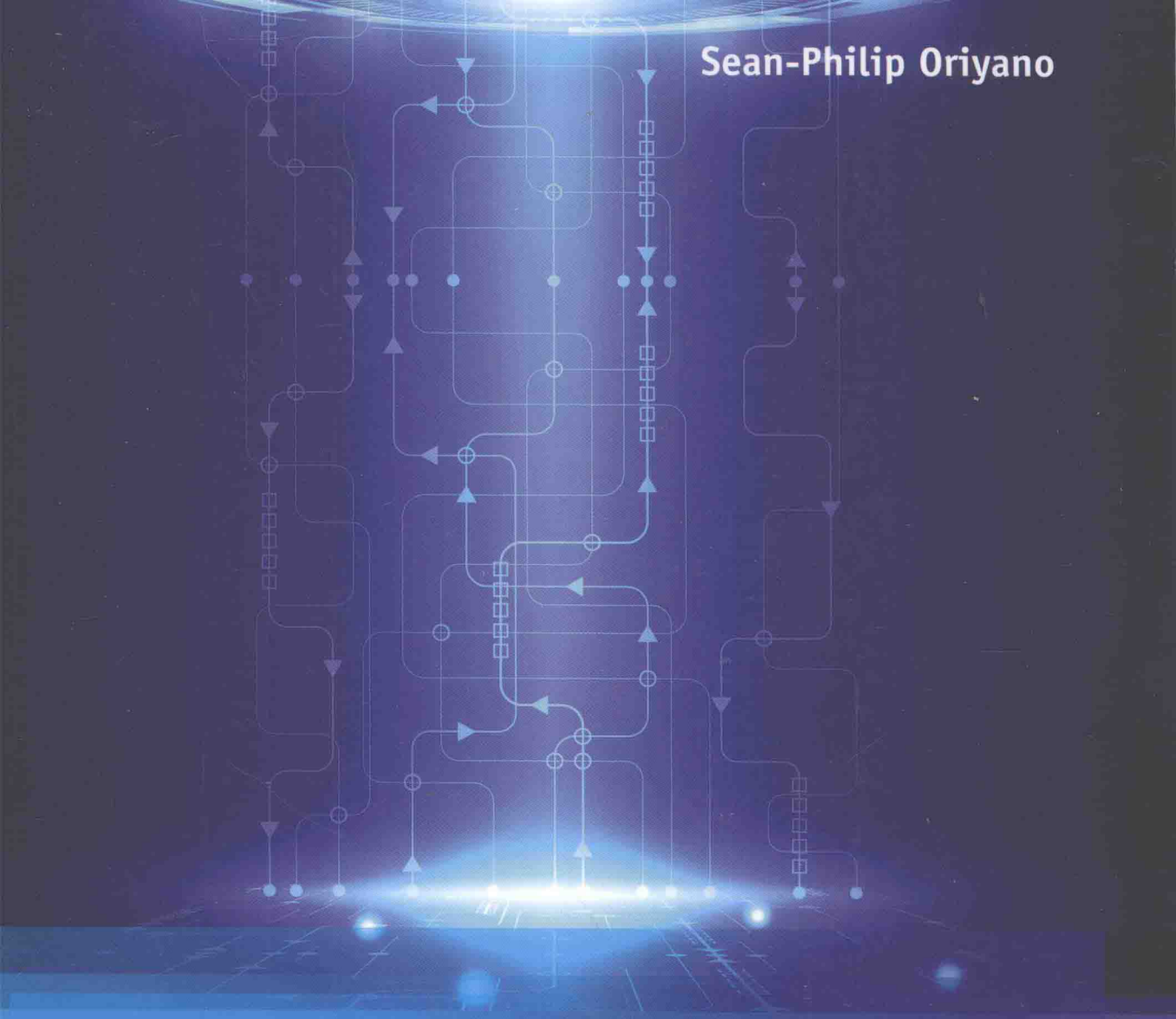

Sean-Philip Oriyano

Penetration Testing

ESSENTIALS

SYBEX
A Wiley Brand

PENETRATION TESTING

ESSENTIALS

Sean-Philip Oriyano

SYBEX®
A Wiley Brand

Development Editor: Kim Wimpsett
Technical Editor: Raymond Blockmon
Production Editor: Christine O'Connor
Copy Editor: Elizabeth Welch
Editorial Manager: Mary Beth Wakefield
Production Manager: Kathleen Wisor
Executive Editor: Jim Minatel
Book Designer: Maureen Forys, Happenstance Type-O-Rama
Proofreader: Josh Chase, Word One New York
Indexer: Ted Laux
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: shutterstock.com/besfoto77

Published simultaneously in Canada
ISBN: 978-1-119-23530-9
ISBN: 978-1-119-32398-3 (ebk.)
ISBN: 978-1-119-23533-0 (ebk.)
Manufactured in the United States of America

Library of Congress Control Number: 2016958766

10 9 8 7 6 5 4 3 2 1

This book is for my Mom and Dad, who instilled in me my core values that have been so valuable in my development as an adult. Although my Dad is no longer with us, I can still feel his influence in everything I do and in fact feel myself sometimes laughing boldly and proudly just like he always used to do. My Mom is still around (and we are keeping it that way), and I am thankful for her support in pushing me to get into science and technology as well as instilling in me a love of sci-fi, bad jokes, and the desire to do the right thing. I love you both. And I first dedicate this book to you.

I also want to dedicate this to the military, which graciously blessed me with the opportunity to attend Officer Candidate School (OCS), even though I was immature and self-centered. While the hell and abuse they put me through sucked at the time, it helped get me on track with my life and realize that I was capable of so much more. It also helped me realize that it's not you that is important; it's the people whose lives you impact. I hope this is something that those of you reading this reflect on. COL K, LtCol A, CPT M, CPT D, CPT J, and CPT A, I am forever grateful for your patience, heart-to-hearts, and straight-up, blunt assessments of me. I hope I have turned into the CW2 that you are proud of. This book is also dedicated to you.

I finally also want to dedicate this book to my staff, who have shown that you can make chicken salad out of chicken poop. You guys have never ceased to amaze me over the last year. You've made me look good, but I refuse to take credit. I didn't do the heavy lifting; you did. I didn't do the improvisation and creativity; you did. I didn't show that what others thought was impossible is indeed possible if you have your act together. I wish I could take credit and say I had something to do with it, but this is all you, and I expect great things from all of you. SSG E, SSG L, SSG S, and CW2 N, keep kicking ass and taking names. I should also take a moment to thank my commander Lt Col L for having faith in my abilities and giving me the support to get things done.

Finally, I want to dedicate this to Lisa. You know who you are and though I have said it many times, I do love you and appreciate you. So deal with it and no flowers or chocolate . . . don't make it weird.

ACKNOWLEDGMENTS

Once again, there are so many people to thank. I sincerely hope I don't forget anyone.

First, thanks to Jim Minatel for the opportunity to do this book, and I look to others in the future.

Second, thanks to Kim Wimpsett. You are without a doubt the primary reason I don't look stupid because of poor language or unclear passages. I really don't know how to say how much I value you as part of the team, and I want you with me on all my future projects.

Third, I have to acknowledge all of the troops of the US military no matter where you are. Though not all of you will make it home (though I sincerely hope you all do), none of you will ever be forgotten, and when I put on my uniform, it is not only for my job but to commemorate your sacrifice.

About the Author

Sean Oriyano is a longtime security professional and entrepreneur. Over the past 25 years he has divided his time between performing security research, consulting, and delivering training both in the field of general IT and cybersecurity. In addition, he has become a best-selling author with many years' experience in both digital and print media. Sean has published several books over the last decade and has expanded his reach even further by appearing on shows on both TV and radio. To date, Sean has appeared on more than a dozen TV programs and radio shows discussing different cybersecurity topics and technologies. When in front of the camera, Sean has been noted for his casual demeanor and praised for his ability to explain complex topics in an easy-to-understand manner.

Outside his own business activities, he is a Chief Warrant Officer (CWO) and commands a unit specializing in cybersecurity, training, development, and strategy. Additionally, as a CWO he is recognized as a subject matter expert in his field and is frequently called upon to provide expertise, training, and mentoring wherever and whenever needed.

When not working, Sean is an avid obstacle course racer and has completed numerous races, a world championship race, and four Spartan Trifectas. He also enjoys traveling, bodybuilding, MMA, Metroid, and "The Legend of Zelda."

INTRODUCTION

Security is one of the topics that gets a lot of attention in today's world. Because of our increasing reliance on different forms of technology, gadgets, and many other types of systems and devices, more attention is being turned to the topic of how secure and safe these devices and systems actually are. In response to the increase in cybercrimes such as identity theft, information theft, disruption of services, hactivism, and even the spectre of terrorism, many organizations—both public and private—face the challenge of having to test, evaluate, and fix potential security issues before they become the victim of a cybercrime as well as potential lawsuits. It is in response to these situations in the past, present, and future that many organizations are scrambling or pursuing various security solutions.

So enters the penetration tester, who represents one of the best and most effective ways of locating, analyzing, presenting, and recommending strategies to reduce potential risk resulting from security incidents. Pentesters are those people who take their in-depth understanding of technology and its vulnerabilities, as well as strengths, and use them at the request of a client to locate and evaluate security problems before those who don't have the organization's best interests at heart.

Who Should Read This Book?

The audience for this book includes those individuals who are already in possession of a technical background and are looking to move into the penetration testing world. Unlike many other books that cover the topic of pen testing, this book strives to introduce you to the topic in a simple and easy-to-understand way. The goal is to help you, as the reader, gain a better understanding of the pen testing process as well as gain experience and knowledge through hands-on exercises and through the exploration of the various theories that form the basis of pen testing.

Upon completion of this book, you should have a better understanding of what it means to be a pentester and the skills, tools, and general knowledge it takes to be successful. Once you finish this book and have practiced what you learned, you will find yourself in possession of the tools needed to pursue more advanced techniques, testing methods, and skills.

What You Need

If you are intending to get the most out of this book, then you should have a few things handy. Before you get started, you should have access to a computer that is capable of running the latest version of Microsoft Windows or Kali Linux that has at least 8 GB of RAM. Additionally, you should have access to virtualization software such as Oracle's VirtualBox or one of VMware's offerings; which virtualization software you choose to use is up to your personal preference and your wallet.

As you read through this book, you will be introduced to a diverse set of hardware and software-based tools used to accomplish a wide array of tasks. When you go through the chapters and exercises, you will be presented with links to download or otherwise acquire the tools of your choosing.

What's Covered in This Book

This book covers a broad range of topics for the beginning pentester. The following is a list of the chapters with a brief description of what each focuses on.

Chapter 1, "Introduction to Penetration Testing": Focuses on the general rationale for penetration testing as well as giving an idea of the skills and knowledge required to be successful.

Chapter 2, "Introduction to Operating Systems and Networking": A firm understanding of the structure of an operating system and the network it attaches to is required to be a pentester. In this chapter, the fundamentals of both are explored in order to establish a foundation to build upon.

Chapter 3, "Introduction to Cryptography": Without cryptography, a lot of the countermeasures used to protect against inadvertent disclosure of information would not work. Additionally, without an understanding of cryptography, meeting various laws and regulations becomes very difficult. In this chapter, a primer on the functioning and mechanics is covered as well as how it is applied.

Chapter 4, "Outlining the Pen Testing Methodology": Pen testing has a process and methodology that must be followed in order to get the most complete and effective results reliably. In this chapter we will cover one of the more popular methods for performing a pen test.

Chapter 5, "Gathering Intelligence": The first step in the process of pen testing is gathering information about your target. In this chapter the various means for gathering information are explored and how they fit in to the overall process.

Chapter 6, "Scanning and Enumeration": Once you have gathered sufficient intelligence about a target, you can start probing and finding out which information can be extracted. Usernames, groups, security policies, and more are on the table in this chapter.

Chapter 7, "Conducting Vulnerability Scanning": Want to take a different approach to finding out about your target? Well, you can use the process of manual or automatic vulnerability scanning to locate weaknesses in an environment for later exploitation.

Chapter 8, "Cracking Passwords": Since passwords are the front line of defense in many environments and applications, time must be allocated to the process of obtaining these valuable pieces of information. Enumeration already gave us usernames, so we can focus on those usernames to gather passwords.

Chapter 9, "Retaining Access with Backdoors and Malware": Investigate, explore, compromise, and now you are in the system. However, once you have gained access and established that beachhead, how do you keep it? In this chapter we will explore precisely that.

Chapter 10, "Reporting": Remember you are working for a client under contract with the goal of finding and reporting on your findings. In this chapter you will see the general format and layout of a report.

Chapter 11, "Working with Defensive and Detection Systems": Of course not all systems are open and waiting to be penetrated. In fact, many systems will have several layers of defense in different forms waiting for you to get in. In this case intrusion detection and prevention systems are your nemesis and here you will learn how to deal with them.

Chapter 12, "Covering Your Tracks and Evading Detection": Leaving clues at the scene of a crime is a sure way to get caught and thwarted. In this chapter you'll learn how to clean up after yourself so hopefully all but the most determined will find you.

Chapter 13, "Detecting and Targeting Wireless": Wireless is ubiquitous and therefore you will have to deal with it in just about any environment you explore. If those environments include mobile devices, you are guaranteed to encounter these networks, which you can then target.

Chapter 14, "Dealing with Mobile Device Security": No matter how you look at it, mobile devices are not only here to stay but they are taking new forms, tasks, form factors, and are part of our everyday lives. Since they have been integrated into the business environment and the lines between business and personal use have been blurred, you must learn how to deal with mobile devices.

Chapter 15, "Performing Social Engineering": In every system there is that one element that represents the weakest link, and in many cases this weakest link is a human being. As a pentester you can use your quick talking, psychology, and clever wording to guide a conversation toward those topics that will give you useful information.

Chapter 16, "Hardening a Host System": Countermeasures of all types are available to slow down or stop an attack. One of the first lines of defense is frequently locking down or hardening a system to reduce the chances of it being compromised

Chapter 17, "Hardening Your Network": Much like with host hardening, countermeasures are available to slow down or stop an attack on networks. Removing protocols, implementing firewalls, and other mechanisms can slow down and frustrate an attacker.

Chapter 18, "Navigating the Path to Job Success": In this chapter, consider yourself a graduate. Now you are looking to a future in penetration testing. This chapter will provide a guide to what to do next to keep developing your skills even further.

Chapter 19, "Building a Test Lab for Penetration Testing": A good pentester needs to practice on equipment that they own. In this chapter we will explore how to set up a basic lab that you can use to practice and experiment.

Contents at a Glance

CONTENTS

CHAPTER 1

Introduction to Penetration Testing

So, you have decided to become a penetration tester (commonly known as a *pentester*). Not sure where to start? This book helps you learn what it means to become a penetration tester and the responsibilities you will be assuming both technically and ethically when you take on this role. You will build the skills necessary to be successful in the world of penetration and hands-on security.

Specifically, you will encounter many hacking methods that are currently being used on the front lines. You will also encounter techniques that you can use during your pen test to gain information or establish a foothold from which to launch more advanced attacks.

In addition, understanding the motivations of hackers can aid you in understanding the scope of an attack or perhaps even aid in discovering details of the attack. In fact, you need to empathize with hackers in order to establish why they may be carrying out an attack and then use that experience to test a client's network.

In this chapter, you'll learn to:

- **Define what penetration testing is and what a pentester does**
- **Learn why you want to preserve confidentiality, integrity, and availability**
- **Appreciate the history of hacking and penetration testing**

Defining Penetration Testing

Being a pentester has become more important in today's world as organizations have had to take a more serious look at their security posture and how to improve it. Several high-profile incidents such as the ones involving retail giant Target and entertainment juggernaut Sony have drawn attention to the need for better trained and more skilled security professionals