PHILLIP L. WYLIE
KIM CRAWLEY

THE PENTESTER BLUEPRINT

STARTING A CAREER AS AN ETHICAL HACKER

WILEY

The Pentester Blueprint

Starting a Career as an Ethical Hacker

Phillip L. Wylie
Kim Crawley

WILEY

Published simultaneously in Canada

ISBN: 978-1-119-68430-5
ISBN: 978-1-119-68435-0 (ebk)
ISBN: 978-1-119-68437-4 (ebk)

Manufactured in the United States of America

Library of Congress Control Number: 2020943760

I dedicate The Pentester Blueprint *to my wife Tiffany and daughter Jordan. Without your love and support, this would not have been possible. As always you support me in my endeavors, encouraging me every step of the way.*

—Phillip L. Wylie

To my loving rock musician boyfriend Jason, my stuffed animal family for assuring me of the rest that I need in order to work effectively, and my late father Michael Crawley for encouraging my very early interest in computers and raising me to write for a living.

— Kim Crawley

About the Authors

Phillip L. Wylie is the Lead Curriculum Developer for Point3 Federal, Adjunct Instructor at Dallas College, and The Pwn School Project founder. Phillip has over 23 years of industry experience in disciplines ranging from system administrator, network security engineer, and application security engineer. He has spent the last eight-plus years as a pentester. During his pentesting career, Phillip has performed pentests of networks, wireless networks, and applications, as well as red team operations and social engineering.

Phillip started his career in pentesting as a consultant, where he spent his first five years. These years gave him experience in various environments for Fortune 500 companies in a broad range of industries. Phillip has a passion for mentoring, educating, and helping others. His passion for education and the cybersecurity community motivated him to start teaching and to found The Pwn School Project, a monthly educational meetup focusing on cybersecurity and ethical hacking. His education efforts, however, expanded beyond the classroom and The Pwn School Project. He can be found routinely giving presentations and teaching workshops at cybersecurity conferences.

Phillip teaches Ethical Hacking and Web Application Pentesting at Dallas College in Dallas, TX. Phillip is a co-host for The Uncommon Journey podcast. Phillip has an associate degree in Computer Networking and holds these cybersecurity certifications: CISSP, NSA-IAM, OSCP, and GWAPT. During his system administrator career, Phillip attained these industry certifications; Microsoft MCSE for Windows NT 4.0 and Windows 2000, Novell CNE, and Cisco CCNA.

Kim Crawley is dedicated to researching and writing about a plethora of cybersecurity issues. Some of the companies Kim has worked for over the years include Sophos, AT&T Cybersecurity, BlackBerry Cylance, Tripwire, and Venafi. All matters red team, blue team, and purple team fascinate her. But she's especially fascinated by malware, social engineering, and advanced persistent threats.

Kim's extracurricular activities include running an online cybersecurity event called DisInfoSec and autistic self-advocacy. When she's not working, Kim loves JRPGs (especially the Persona series), trying to cook Japanese and Korean dishes, goth music and fashion, and falling down Wikipedia and TV Tropes rabbit holes.

Acknowledgments

I thank all of my students and the people I have mentored over the years: You helped me realize my passion for teaching. I thank my friend and fellow adjunct instructor Jason Alvarado for hiring me to teach at Dallas College (formerly Richland College). Teaching Ethical Hacking and Web Application Pentesting helped me discover my love for teaching, which has opened so many doors. I thank my friend and Dallas Hackers Association founder Wirefall for your friendship and for founding the Dallas Hackers Association.

The Dallas Hackers Association was pivotal in getting me involved in the hacking and cybersecurity community. This led to speaking and teaching workshops at cybersecurity conferences, where I have connected with so many amazing people. Thanks to Wirefall, I met Marcus Carey, the author of the *Tribe of Hackers* book series (Wiley, 2019). Thanks to Marcus for including me in the *Tribe of Hackers Red Team* book, which has been very helpful in my career and ultimately led to my being offered the opportunity to write this book. I acknowledge Marcus for his contributions to the cybersecurity community and for his efforts for the betterment of our world and for inspiring me to make the world a better place.

Last, but definitively not least, I thank Kim Crawley, my amazing coauthor, who helped me take my conference talk from conception to a book. Thanks for helping me take an idea—28 PowerPoint slides—and breathing life into it.

I would like to thank my friend, Rhea Santos for taking time out of her schedule to create the artwork for the chapters of the book. Rhea is a friend and someone that I have taught and mentored. It is so fitting to have her art in The Pentester Blueprint since it was the people that I taught and mentored that inspired me to write this book.

Thanks also go to Jim Minatel at Wiley for the opportunity to write this book and to Gary Schwartz and the rest of the Wiley staff for making this book a reality. Your hard work is much appreciated.

—Phillip L. Wylie

I'm tremendously grateful to Phillip Wylie for inviting me to collaborate with him on *The Pentester Blueprint*. Phil developed a great Pentester Blueprint curriculum, which he has perfected while teaching it in workshops and schools

across the United States. This book brings that curriculum to the masses while adding some of my own ideas. Many, many ethical hackers have been born from Phil's generosity with his expertise! Phil, you've been a pleasure to work with, and I look forward to working with you again on future projects.

I also thank Gary Schwartz for being such a patient editor. This book has benefited greatly from your work behind the scenes. I also enjoyed our funny discussions of popular culture over email.

I thank Jim Minatel, Associate Publisher at Wiley, for also being vital to the success of this book. I really appreciate your encouragement of my work. I shine with the support of publishing professionals like you.

I thank Victoria Lamont, my loving sister and the only blood relative left in my life. Although you say you don't understand my technical jargon, you've been very supportive of my cybersecurity research and writing career. Thank you so much for everything you do!

On that note, I thank my de facto "parents-in-law" Joe and Laurie, and Rose. You always make Christmas special for me. Jason, I look forward to giving you autographed copies of this book.

Thank you Olena, for being such a supportive friend.

I thank Bora's Joe Pettit and David Turner, well-known names in the world of tech marketing. You both took a chance on me and helped to start the career that I enjoy today. I'm eternally grateful, because getting your foot in the door is always the hardest part of establishing a career.

I thank Marcus Carey. Not only did you write an excellent foreword to this book, you also do great work helping people get into the cybersecurity field. I'm doing my best to read all of your books! It was also an honor to be included in your first volume of *Tribe of Hackers*.

Finally, I thank my boyfriend Jason, once again. I listen to your music whenever I miss you, and I always look forward to spending time with you in my apartment or yours, once a week. Your encouragement of me during this successful period of my life is always appreciated. I love you, darling.

— Kim Crawley

Contents at a Glance

Contents

Foreword

I'd say the most coveted positions in cybersecurity and information technology as a whole are roles as penetration testers, or *pentesters*, also known as *ethical hackers*. I want to emphasize the ethical part of that last sentence. There are many that go down the path of self-study, trying to get into the field, who end up crossing the line into unethical and even illegal behavior.

Remember always to use your superpowers for good. Funny enough, when people find out that I'm an ethical hacker, many ask me to break into something for them. They also ask how they can learn what I know so that they can get a cool job. I certainly will point them to two books that I co-authored with Jennifer Jin, *Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World* and *Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity,* both published by Wiley in 2019, to which my friends Kim Crawley and Phillip Wylie contributed.

If I were to point someone trying to get into this line of work, I'd most certainly point them to Phillip Wylie. Phillip is the only person I know that can teach you how to break into a company ethically for security purposes and to have wrestled a bear and lived to talk about it. Like many of our backgrounds, Phillip's was unique and something that should be embraced. There is no one correct path to be a penetration tester.

Phillip continues to pay it forward by helping tons of people to learn about ethical hacking and volunteering hundreds of hours helping people learn. You will learn a lot from this book, and I'm going to ask you a favor: Please pay it forward and help someone else by teaching them something that you already know or learn from this book which can help them out.

I just want to thank Phillip for being such a blessing to so many people. I hope you learn a lot or even fill in some blanks in your knowledge. I wish you an abundance of success on your journey.

Marcus J. Carey
Creator of Tribe of Hackers Series

Introduction

The Pentester Blueprint was born from ethical hacker Phillip Wylie's excellent pentesting curriculum of the same name. Whether or not you're able to attend one of the many workshops and classes that Phil gives every year, this book will teach you not only how to become a pentester but also how to become a successfully employed pentester! By reading this book, you have started the journey on your ethical hacking career. The future looks bright for you!

How I Became a Pentester

"My journey to becoming a pentester started with my first IT job as a system administrator. In my previous career as a draftsman, I learned about the system administrator role. It intrigued me and seemed more interesting that creating drawings on AutoCAD. I taught myself how to build computers and about a year later I took a certified NetWare engineer (CNE) certification course and learned the Novell NetWare network operating system. Not long after completing the course I got my first system administrator job and spent a little over six years in that IT discipline. I got interested in information security three years into my system administrator career and later moved into a network security role at the company where I worked. One and a half years later I became part of a newly formed two person application security team. I got to learn how to use web application vulnerability scanners and learned about penetration testing, which became my next career move. Almost seven years later I was part of a layoff and was fortunate enough to land my first penetration testing job working as a consultant for a cyber security consulting company. That was the start of my eight and a half penetration testing career."