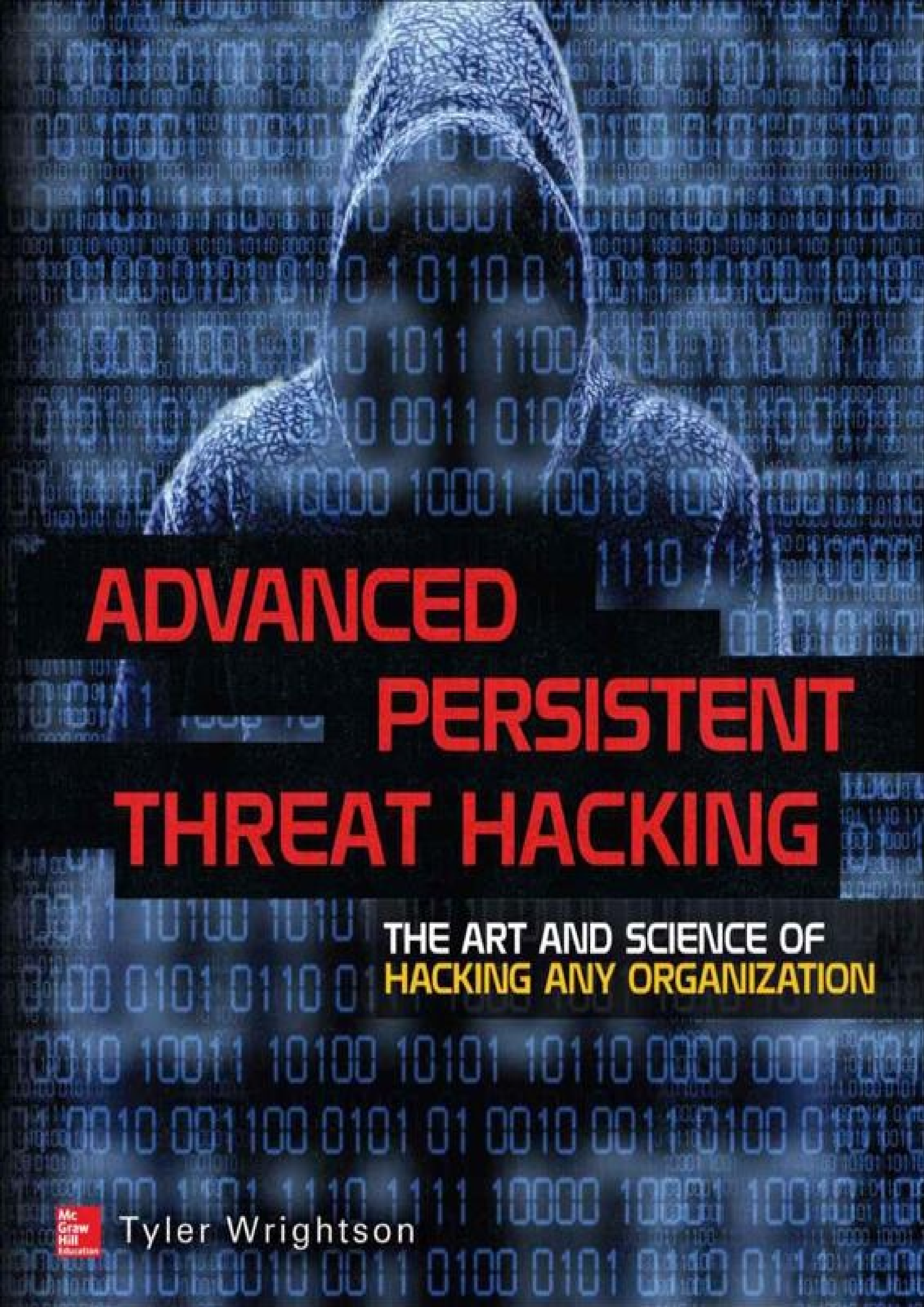

ADVANCED PERSISTENT THREAT HACKING

THE ART AND SCIENCE OF HACKING ANY ORGANIZATION

Tyler Wrightson

About the Author

Tyler Wrightson is the author of *Advanced Persistent Threats* as well as *Wireless Network Security: A Beginner's Guide*. Tyler is the founder and president of Leet Systems, which provides offensive security services such as penetration testing and red teaming to secure organizations against real-world attackers. Tyler has over 13 years' experience in the IT security field, with extensive experience in all forms of offensive security and penetration testing. He holds industry certifications for CISSP, CCSP, CCNA, CCDA, and MCSE. Tyler has also taught classes for CCNA certification, wireless security, and network security. He has been a frequent speaker at industry conferences, including Derbycon, BSides, Rochester Security Summit, NYS Cyber Security Conference, ISACA, ISSA, and others. Follow his security blog at http://blog.leetsys.com.

About the Technical Editors

Reg Harnish is an entrepreneur, speaker, security specialist, and the chief security strategist for GreyCastle Security. Reg has nearly 15 years of security experience, specializing in security solutions for financial services, healthcare, higher education, and other industries. His security expertise ranges from risk management, incident response, and regulatory compliance to network, application, and physical security. Reg brings a unique, thought-provoking perspective to his work, and he strives to promote awareness, establish security fundamentals, and reduce risk for GreyCastle Security clients.

Reg attended Rensselaer Polytechnic Institute in Troy, New York, and has achieved numerous security and industry certifications. He is a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), and a Certified Information Systems Auditor (CISA). In addition, Reg is certified in Information Technology Infrastructure Library (ITIL) Service Essentials. He is a member of InfraGard, the Information Systems Audit and Control Association (ISACA), and the Information Systems Security Association (ISSA). In addition to deep expertise in information security, Reg has achieved numerous physical security certifications, including firearms instruction, range safety, and personal protection.

Reg is a frequent speaker and has presented at prominent events, including US Cyber Crime, Symantec Vision, ISACA, ISSA, InfraGard, and more. His successes have been featured in several leading industry journals, including *Software Magazine*, *ComputerWorld*, and *InfoWorld*.

Comrade has been in information security since the early 2000s. Comrade holds several industry certifications, but believes the only one that really means anything in regard to this book is the OSCP certification by the Offensive Security team. He currently performs penetration testing against all attack vectors, network, application, physical, social, etc., for clients in all verticals, including many Fortune 500 companies.

Advanced Persistent Threat Hacking

The Art and Science of Hacking Any Organization

Tyler Wrightson

Mc Graw Hill Education

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

ISBN: 978-0-07-182837-6
MHID: 0-07-182837-0

The material in this eBook also appears in the print version of this title: ISBN: 978-0-07-182836-9, MHID: 0-07-182836-2.

eBook conversion by codeMantra
Version 1.0

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

TERMS OF USE

LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

To my father and to my mother and stepfather.
For putting up with the adolescent headaches and being supportive even of "nontraditional" hobbies.

And to Erin.

The love of my life.

For whom I do everything.

Contents at a Glance

Contents

Acknowledgments

There are so many people I want to acknowledge and thank—whether you have helped me directly with this book or are just a good friend, I'm glad to have you all share this with me. First, I have to thank Erin. I love you so much, thank you for all of your unending support. I have to thank my mother for being a great mother, a wonderful person and woman, super supportive and loving, always understanding, and the best mom ever. I want to thank my stepfather for providing good stories, a level head, and plenty of cognac to a much-younger Tyler.

I want to thank my father for being a great father, a role-model gentleman, and the best daddio ever. Thank you to my future stepmother for making my dad very happy and being a genuinely great person.

Thank you to Raeby for being the best little big sister, (usually) level headed, but always loving and a little rock in my memory. Thank you to Donby for the endless artistic support, being a great brother-in-law, and providing us with the best niece in the world.

Jenners, for always being excited and supportive, and the best little sister. Corby, for being a good and kind person and a great brother. Bren, for being a little punk, but a good person and a great brother. I love you all.

Thank you to all my friends who I couldn't hang out with on more than a few occasions.

Thank you, Reg, for all of the help to make this book what I wanted it to be and all the fun and education working together. I really did learn a lot working with you. Thank you, Stamas, for all the good times, being a great teammate, and being a really sweet guy no matter how much you try to hide it. We'll definitely work together in the future.

Thank you, Steve and Bob, for being a huge help in so many different ways. I really can't thank you enough. You've gone well beyond what was necessary so many times, and it's been really awesome working with you.

I have to thank Stacks Espresso for not only providing a great place to do an absurd amount of the writing for this book, but also providing the necessary caffeine to do it. Thank you to my new team at Stacks: Ron, Lacy, Kevin, Jess, Jammella and John for being awesome and making this a really enjoyable experience.

Thank you, Elo, for all the direct and indirect help. I'm so glad the fear of losing a vital organ didn't stop us from becoming friends. It's been awesome sharing this love for hacking and this awesome security journey with you. I love you no matter how much of a pain in the ass you are.

Last but absolutely not least, I have to thank everyone at McGraw-Hill Education who helped make this book. Amy Jollymore, for seeing the vision and concept very

early on. Brandi Shailer, for truly helping me through so many issues and deadlines; many, many phone calls; and an absurd amount of e-mails. Amanda Russell, for all your help and support. Thank you all so much.

Introduction

Writing this book was a far more difficult task than I realized when I first set out. This book has actually been well over a decade in the making. Starting out as a simple thought experiment to determine how I might be able to hack into any organization, over the years, it turned into more of an obsession.

Finally, after many years of penetration testing, I felt that not only did I have a solid game plan to successfully hack even the most secure organizations, but I also had plenty of firsthand experience that gave me my own unique perspective.

Why This Book?

This book was written with one crystalized purpose: to prove that regardless of the defenses in place, any organization can have their most valuable assets stolen due to the complete immersion of technology with our world. The truly alarming fact is that not only is this possible, but it is probably far easier than most people realize.

Who Should Read This Book?

This book was originally written for anyone tasked with ensuring the security of their organization, from the CSO to junior systems administrators. However, much of the book will provide enlightening information for anyone even remotely interested in security.

The people who will most likely gain the most from this book are the foot soldiers who must make tactical security decisions every day. People like penetration testers, systems administrators, network engineers, even physical security personnel will find this book particularly helpful. However, even security managers and C-level personnel will find much of this information enlightening.

What This Book Covers

This book starts out at a very high level and quickly gets into the nitty-gritty of attacking an organization and exploiting specific vulnerabilities. These examples are meant to be actionable, hands-on examples that you can test yourself. However, it’s critical to understand that in no way should this book be considered to contain every detail that is necessary to hack any organization. Hopefully, every reader understands that to contain every detail, this book would quickly reach a size that would not fit on any bookshelf. Instead, in an attempt to find balance, many things that are believed to have been covered adequately by other books or that are assumed to be known by a reader with a moderate understanding of hacking have been left out of this book.

In an attempt to give the most real, unabashed, and meaningful perspective, there has been no tiptoeing around sensitive subjects, and nothing has been held from this book for fear of being too controversial. This book has been written from the perspective of a criminal, with no other goal than to take your organization's most meaningful assets by any means necessary (aside from violence).

It is only with this perspective that we can meet Sun Tzu's tenet of knowing thy enemy. And with that perspective begin to adequately defend against these types of threats.

It is also important to understand the difference between the typical use of the word APT and the meaning in this book. In this book, I attempt to commandeer the term APT to define a new type of hacker able to infiltrate any organization despite a very small budget and surprisingly with very accessible skills. As always with everything I do, there may be a small dash of tongue-in-cheek humor.

How Is This Book Organized?

In the first part, we stick to the high-level concepts that make every organization vulnerable. In Chapter 2, we discuss a few interesting real-world examples of both unsophisticated and sophisticated threats.

In Chapter 3, we discuss the methodology you must follow to become capable of hacking any organization. This methodology includes a few hard-set technical skills that you must obtain; however, it is primarily dominated by the correct system and mental constructs necessary to hack any organization.

Chapters 4 and 5 dive into the first tactical steps in the methodology and cover in detail the technical and nontechnical types of data you should attempt to obtain about your target through active and passive reconnaissance.

Chapter 6 begins with an in-depth discussion of strategic and tactical components of effective social engineering. This is followed by tactical examples of spear phishing a target through remote technical means such as e-mail and building effective phishing websites.

Chapter 7 moves on to targeting remote users at their homes and other locations. This chapter focuses primarily on exploiting wireless vulnerabilities that can allow us to easily and anonymously exploit these users. This includes targeting wireless networks and vulnerabilities, as well as creating the most effective rogue access points and exploiting wireless clients and communications.

Chapter 8 demonstrates how to create and use traditional audio, video, and GPS bugs to monitor key locations and individuals. This is followed by details on how to create and program next-generation hardware-based backdoors such as the Teensy device, as well as backdoored hardware such as laptops and smart phones.

Chapter 9 goes in depth into circumventing many of the most common physical security controls and physically infiltrating target locations. Copious examples and useable tools and techniques are covered in detail.

Finally, Chapter 10 closes with a discussion of the types of software backdoors that can be used throughout all of the previous attack phases to maximize the effectiveness of any attack. This includes code examples as well as functionality that may seem somewhat low tech but will provide great results.

1
CHAPTER

Introduction

You didn't realize it, but when you decided to use the Internet, a computer, that new cell phone, even Facebook and Twitter, you joined a war. Whether you know it or not, this is war and it's making us all soldiers. Some of us are peasants with pitchforks, and others are secret agents with sniper rifles and atom bombs.

In the past, when a bank had to account for security, they only had to worry about physical threats and tangible people. Nowadays, American banks are being attacked by intruders from countries with unfamiliar names who utilize attacks that exist only digitally, in electricity, transistors, 1's and 0's. Businesses as old as dirt have to deal with twenty-first century invisible, ethereal, and complicated threats. How well do you think they're holding up? Many systems and controls are available to deal with physical threats, including the law. In the past, if you were caught trying to rob a bank, you could spend serious time in prison, as there are laws that make this illegal. Unfortunately, American law is struggling to deal with this constant barrage of foreign attackers. In addition, the Internet makes it possible for an attacker to appear to originate from any country he wishes.

In the modern digital era, everyone connected to the Internet is under constant attack, both businesses and home users. Is there a purpose to this barrage of attacks? Many times, the people compromised are just random victims of criminals who want to steal as much data as possible, package it up, and sell it to the highest bidder.

"But I don't have any data that's valuable to a criminal." This is such a common statement from people who don't understand the threats, their capabilities, or their motives. Of course, a criminal doesn't really care about your apple pie recipe or your vacation pictures, but even with zero data, your computer *resources* are still valuable to an attacker. A compromised computer represents another processor to attempt to crack passwords, send spam e-mail, or another host to help knock down a target in a distributed denial of service (DDoS) attack.

This world has become a playground for *anyone* who understands technology and is willing to bend the rules. By manipulating technology or people in unanticipated ways, an attacker is able to accomplish the seemingly impossible. This doesn't just include criminals, although the criminal element is huge, pervasive, and only increasing in efficacy—*anyone* can put in the time to learn about our technology-warped world. We now live in an age where anything is possible. In Chapter 2, you'll see real-world examples demonstrating some interesting and enlightening examples.

For those who understand technology, we live in an extremely interesting time. We're reminded on an almost daily basis of the struggles of corporations by headlines alerting us to the latest breach. Major parts of the American infrastructure have been called "indefensible" by those tasked with ensuring its security, and nation-states have