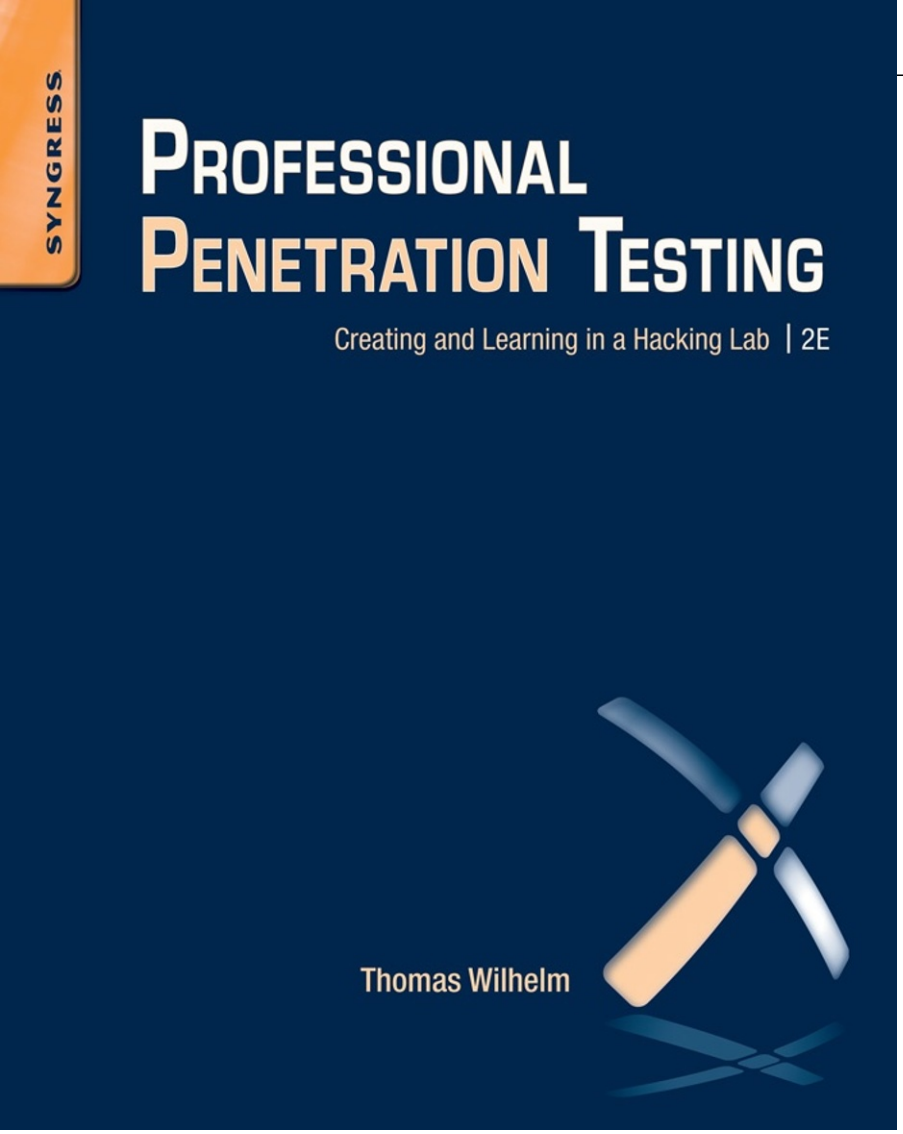
SYNGRESS
PROFESSIONAL
PENETRATION TESTING
Creating and Learning in a Hacking Lab | 2E
Thomas Wilhelm

Professional Penetration Testing

Intentionally left as blank

Professional Penetration Testing

Second Edition

Creating and Learning in a Hacking Lab

Thomas Wilhelm

Matthew Neely, Technical Editor

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an Imprint of Elsevier

SYNGRESS®

Acquiring Editor: *Chris Katsaropoulos*
Development Editor: *Heather Scherer*
Project Manager: *Malathi Samayan*
Designer: *Matthew Limbert*

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

First edition 2009

Library of Congress Cataloging-in-Publication Data
Wilhelm, Thomas.
Professional penetration testing / Thomas Wilhelm. – Second edition.
volumes cm
Includes bibliographical references and index.
ISBN 978-1-59749-993-4 (alkaline paper)
1. Computer networks–Security measures. 2. Penetration testing (Computer security) 3. Computer networks–Testing. 4. Computer hackers. I. Title.
TK5105.59.W544 2013
005.8–dc23 2013016650

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-59749-993-4

Printed in the United States of America
13 14 15 12 11 10 9 8 7 6 5 4 3 2 1

For information on all Syngress publications, visit our website at *www.syngress.com*

Contents

Preface

It is amazing how much has changed in the few years since I wrote the first edition of this book! This revision includes a lot of new material—not simply a patchwork of updated material extracted from the first edition. I listened to all my readers and reformatted quite a bit of the material so it reads better, and fattened quite a bit of the content to expand or add to the concepts discussed in the first edition. I hope you all enjoy it!

This edition is also different in that we did not include a companion DVD. All the additional material that would have been included is available at HackingDojo.com and referenced heavily within this edition. This will allow updates to occur between this edition and the next one, as new material/pentesting targets/pentesting platforms are released. If you have any questions or comments about the book, its contents, or the HackingDojo.net site, please don't hesitate to contact me directly at info@HackingDojo.com.

Enjoy!

Thomas Wilhelm

Intentionally left as blank

About the Author

Thomas Wilhelm has been involved in Information Security since 1990, where he served in the U.S. Army for 8 years as a Signals Intelligence Analyst/Russian Linguist/Cryptanalyst. A speaker at security conferences across the United States, including DefCon, HOPE, and CSI, he has been employed by Fortune 100 companies to conduct risk assessments, participate and lead in external and internal penetration testing efforts, and manage Information Systems Security projects. Thomas is also an Information Technology Doctoral student who holds Masters degrees in both Computer Science and Management. Additionally, he dedicates some of his time as an Associate Professor at Colorado Technical University and has contributed to multiple publications, including both magazines and books. Thomas currently performs security training courses for both civilian and government personnel through HackingDojo.com and maintains the following security certifications: ISSMP, CISSP, SCSECA, and SCNA.

Intentionally left as blank

About the Technical Editor

Matthew Neely (CISSP, CTGA) is the Director of Research, Innovation, and Strategic Initiatives at SecureState, a security management consulting firm. At SecureState, Matt leads the Research and Innovation team which focuses on imagining, researching, and developing tools and methodologies which address the challenging problems of the information security industry. Prior to becoming the Director of Research, Innovation, and Strategic Initiatives, he served as the Vice President of Consulting and Manager of the Profiling Team. His research interests include the convergence of physical and logical security, lock and lock picking, cryptography, and all things wireless.

Intentionally left as blank

Acknowledgments

Family

Although a revision is theoretically easier than writing a new book, the reality is there is really no reduction in effort. Again, my family has been fantastic in supporting my endeavor to update this book and provided me with additional guidance along the way. Again, I dedicate this new, revised book to my loving wife Crystal, who has been supportive in everything I do… not just writing.

HackingDojo.com

Since I migrated the learning material off Heorot.net to HackingDojo.com, I have met a lot of really neat people. I would like to thank them personally as well, since we learned a lot together—they have brought many new ideas and thoughts to the training sessions, which have pushed me to find new and innovative ways to perform pentests. Besides that, I consider most of them friends, since we have gone beyond the simple student-teacher relationship. Thanks to you all!

On the Side

Although I would like to include everyone who has helped me along the way, in this edition I would like to thank all those people who have helped me make the "Be the Match" drive at DefCon the past few years become a real success. We have had such a turnout of people signing up to become potential stem cell donors that I would like to send out this special message to all those who have signed up or spread the word—thank you from the bottom of my heart. You are all doing something very special, and the world is a better place because of your willingness to help others.

Intentionally left as blank

CHAPTER 1

Introduction

CONTENTS

CHAPTER POINTS

- Introduction
- About the Edition
- Download Links and Support Files
- Summary

INTRODUCTION

Even though it has been only a few years since writing the previous edition of "Professional Penetration Testing," so much has changed in the field that it's time to update and expand. The ultimate truth of pentesting is that system and network security is a constantly moving target, and many new resources have been made available to those interested in becoming professional penetration testers. In this second edition, we will take a look at some of the changes that have occurred, and go into more detail on how to conduct pentests—both internally and externally.

The feedback on the previous edition includes a lot of praise for what I had written before—the writing style, the exercises in the back of each chapter, and the coverage of the material, just to name a few. However, there were also those who wanted more—in-depth coverage of the different attacks, more complex lab setups, and a greater number of examples; again, just to name a few. This edition plans on making that happen.

Another change that has occurred in the past few years is the explosion of e-books. Numerous copies of my previous edition have been sold and sent electronically. Previously, a DVD had been included with the physical book, which could not (obviously) be included with the e-book version. Starting with this edition, all material that would have been included in the new DVD will be available for download on a support Web site (HackingDojo.com). This provides the additional benefit of adding corrections and relevant feedback for the readers when identified, instead of having to wait for another printing to make the changes.

The last major change that I have made to this title is we will restrict most of our activities and attacks to our labs. Previously, examples were included that reached onto the Internet and interacted with online resources. However, we will attempt to demonstrate all the attacks, examined in these books, within the confines of a lab (we won't be 100% successful, but we will try to get as close to that percentage as possible). This includes some of the more complex attacks, such as those conducted against hardware devices within a network. This was definitely a challenge; but it was extremely important to try and isolate the attacks to a preconfigured lab so that the readers would be able to recreate the examples given in the book successfully. In order for the readers to be able to follow along with the examples in this book, configuration data will be available on the companion Web site for download and installation.

I am really excited about the changes made to this series, and hope it helps you maximize your learning within the field of professional penetration testing … let's begin!

ABOUT THIS EDITION

Besides the increase of pages within this title, there is a greater purpose behind this edition. In the last edition, all attacks were treated the same, regardless of whether the pentest was conducted externally (targeting Internet-facing systems) or internally (conducted within the organization's network as if we were a malicious "insider"). Additionally, we meshed different techniques with disparate skill levels into the mix, making it difficult for some readers who were attempting to grasp "where to begin." In this book, we will modify the layout

significantly in such a way that readers who have different skill levels can begin at different stages within the book, allowing them to both learn and practice those specific techniques in which they need to focus.

The first eight chapters concentrate primarily on the following—getting set up with a basic lab, learning the methodology behind conducting pentests, and learning the techniques necessary to conduct external pentests. Most of the remaining chapters not only expand on some of these same concepts but also focus on what to do during an internal pentest, including network appliance attacks, wireless hacking, and man-in-the-middle attacks. I saved the last couple of chapters to chat about reporting and to answer questions and motivate readers on how they can become professional penetration testers. So let's discuss specifics and break down what is covered in each chapter of both books.

Getting Setup

As part of any important discussion regarding hacking, we dive straight into the discussion of right and wrong. We start out with a discussion of "Ethics and Hacking" (Chapter 2). The reasons to stay ethical as a professional penetration tester still outweigh excuses to stray into any sort of malicious activity, so we will take a look at some of the different ethical standards that exist and laws that guide and restrict our actions during the testing itself. Although a topic most people tend to skim over, ethics is a critical topic within corporations today, and by understanding how to conduct ourselves during pentest projects, we can work to improve our professional relationships with both clients and employers.

Chapter 3, titled "Setting Up Your Lab," begins with how to set up a basic, yet very functional, virtual lab. One of the more frequent questions received by individuals beginning their journey into professional penetration testing is "What equipment do I need to set up a lab," followed by "How do I learn to hack?" We will set up a quick-and-easy lab using a virtual network, so the reader can be on their way to solving both questions. We will also look at different virtual systems that we can include in the lab, each providing different challenges and learning opportunities. Once we have the basics down, we discuss how to set up more elaborate labs that mirror corporate computer environments, so we can test more advanced topics. We will examine how to set up actual network devices, such as switches and routers. Configuration for these systems will be provided on the supporting Web site so that the reader can again replicate what is demonstrated within these pages. The purpose behind this upgrade to our pentest lab is to introduce some of the most effective methods in obtaining access to systems and network devices—methods that could make or break a pentest.

Chapter 4, "Methodologies and Frameworks," examines the more well known and accepted standards and procedures used during professional penetration testing. The industry has advanced leaps and bounds over the past 20 years, and work to codify the higher arching procedures within pentesting has been mostly achieved (there is still a lot of work to do, but it's more fine-tuning now as opposed to complete rewrites). In this chapter, we discuss a couple options and examine some of the advantages and disadvantages of different methodologies.

Chapter 5 covers how to run a project. Titled "Pentest Project Management," this chapter will be a bit different than in the previous edition. In this volume, we will again discuss how to manage pentesting within an organization; however, we will also discuss how to manage a pentest as a solo consultant, without the support of larger, corporate infrastructure.

Performing the Penetration Test

The next handful of chapters will deal with the specifics within the methodologies discussed in Chapter 4, "Methodologies and Frameworks." The actual steps to identify exploitable vulnerabilities, compromise systems, and elevate privileges are typically those tasks usually associated with penetration testing.

In Chapter 6, "Information Gathering," although the exact terminology differs within different publications, we will examine both passive and active information gathering techniques, which will be used to provide guidance during the initial phases of the penetration test. Depending on our needs during the project, we may need to include stealth into our activities; we will see how to do both using both techniques.

Chapter 7, "Vulnerability Identification," builds on our discussion of information gathering. In this chapter, we will examine port scanning tools and techniques, system and service identification, and finally vulnerability identification. We will also discuss the difference between what auditors do and what pentest engineers do during this phase, which distinguishes these two professions from each other.

Chapter 8, titled "Vulnerability Exploitation," is probably the more difficult topic to discuss in this volume because of the fluidity of different exploitation techniques. We will cover a variety of different attacks so that the reader can get a feel for the extremely varying methods used to exploit systems. We will also examine some automated tools as well and discuss exactly when they should be used and when not to use them.

Once we finish these chapters, we will gradually shift our main focus and look at things from a more internal-centric focus.

Internal Pentesting

In the next few chapters, we continue our examination of how to conduct a penetration test. We start with Chapter 9, "Local System Attacks," in which we start finding ways to extract information from within a compromised system; it may not always be possible to exploit a system and immediately have root/administrator access.

Chapter 10, "Privilege Escalation," differentiates and details both remote and local password attacks, and the advantages and pitfalls with each. We will discuss how to obtain the appropriate wordlists needed to conduct dictionary attacks and examine how to "mangle" our dictionaries to expose additional user passwords. We also discuss ways to elevate privileges within compromised systems.

Chapter 11, "Targeting Support Systems," focuses on those systems and applications found within an organization, including domain name and distributed directory information. By attacking the support systems, we can better understand the purpose of the network, and systems included within the network.

Chapter 12 discusses "Targeting the Network," which allows us to intercept data between systems or devices. In this chapter, we will look at how to conduct layer 2 man-in-the-middle attacks to obtain sensitive information at the higher levels within a data stream. Another focus of this chapter will be on exploiting the network devices within our target network, to include routers and switches. We also delve into the concept of attacking wireless networks, which briefly discusses the techniques used to penetration wireless access points. Once compromised, we see what we can discover listening to the data traversing the wireless network as well as seeing what other network attacks we can conduct.

Chapter 13 touches on the concept of "Web Application Attack Techniques." A topic that rightly deserves (or shall we say requires) its own book; we will examine those more common attack techniques that expose data within a Web site or circumvent access controls. We will also discuss default files and other findings that may not directly contribute to exploitation of the target system but may provide us with useful information nonetheless.

Personal Skills

Chapter 14, titled "Reporting Results," deals with how to write up a document and provide the appropriate risk metrics for a client, so they can mitigate their security vulnerabilities appropriately. We will discuss different resources available to provide the documentation and metrics to a client, in addition to methods to generate our own.