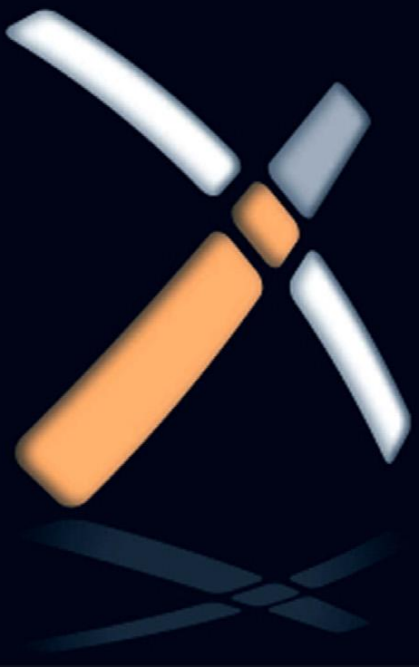
SYNGRESS

Penetration Tester's Open Source Toolkit

Third Edition



Jeremy Faircloth

Penetration Tester's Open Source Toolkit

This page intentionally left blank

Penetration Tester's Open Source Toolkit

Third Edition

Jeremy Faircloth

Neil Fryer, Technical Editor

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

Syngress is an imprint of Elsevier

SYNGRESS

Acquiring Editor: Angelina Ward
Development Editor: Matt Cater
Project Manager: Paul Gottehrer
Designer: Alisa Andreola

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

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Application submitted

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

ISBN: 978-1-59749-627-8

Printed in the United States of America

11 12 13 14 15 10 9 8 7 6 5 4 3 2 1

Dedication

To my Mother-in-Law, Susan Gonzales

As an author, it is difficult to pick any one person to dedicate your work to as there are always so many people who have an impact on your life and deserve recognition. In my case, I'd like to dedicate this book to someone who was always able to see the future.

I grew up in a small town in New Mexico where I attended school and became best friends with the girl who would later become my wife. Her mother was a teacher at our school and was always kind to the geeky kid hanging out with her daughter. I have many memories of catching a lift with my best friend Christina and her mom, Sue, when it was cold outside. Even then, Sue always told me that I should never give up on my dreams and never let anyone tell me that there is something that I can't accomplish. She told me that in time, I would always succeed (prediction #1).

Years later, I asked Christina if she would be my wife and she tearfully accepted my proposal. The next step, as it is for many engaged couples, is to tell our respective families about our decision. When we told my future mother-in-law Sue, she didn't react with surprise or anger. Instead, she said to my newly betrothed, "I told you so." Apparently she had predicted to my future bride far in advance that I was the one she was destined to marry (prediction #2).

After our wedding, my mother-in-law continued to be a positive influence in our lives and was always a willing ear for my wife when I was working long hours or traveling for my job. She taught my wife independence when she was a child and as an adult helped her learn how to deal with the trials and tribulations of living with a professional geek. Without that, I don't know that my wife would be able to handle the unique lifestyle that comes with this type of work.

This week four years ago, my mother-in-law, Susan Gonzales passed away. She is no longer with us in body, but her legacy lives on in her daughter and through the lessons that she taught both of us. This book would not exist if Sue had not been in our lives, so I am proud to have this opportunity to dedicate it to her.

Mom, we love you and miss you very much.

Jeremy Faircloth

This page intentionally left blank

Contents

This page intentionally left blank

Acknowledgments

From start to finish, this book has taken a year of effort and has been built upon the death of two keyboards, a laptop, and various other hardware components. It also involved a tremendous amount of bandwidth and many late nights trying to get a tool to do exactly what it's supposed to when the technology involved is conspiring to make things difficult.

All joking aside, no effort of this magnitude can be accomplished in a vacuum and I am very grateful to a number of people for making this possible. First and foremost to my family for putting up with me while I've been working on this. My wife Christina and my son Austin are two of the most understanding people in the world and have immeasurable patience when it comes to putting up with me and my passion for technology and teaching. Christina and Austin, thank you for helping me make this a reality. The biggest sacrifice made to get this book done has been your time with me and I appreciate you both being willing to make that sacrifice so that this book could be written.

Thank you also to Matt Cater, Rachel Roumeliotis, and Angelina Ward with Syngress for giving me the opportunity to do this project and providing help, advice, feedback, and support throughout the entire process. This wouldn't be possible without publishers like Syngress who allow us technical authors the chance to get our words on paper and out to the world. I have been contributing to Syngress books since 2001 and the experiences I've had doing this over the last decade have always been outstanding.

At its foundation, this book is about open source tools. A huge thank you has to go out to the open source community and the security researchers who contribute their knowledge and time to that community. In the distant past, security professionals held their secrets close to the chest and didn't share because they were afraid that they'd lose their technical edge if they disseminated their knowledge. Fortunately, as a community we've learned that sharing doesn't diminish us, but instead gives the opportunity for others to enhance what we've done and improve on our work. So to everyone in the open source community, thank you. This book wouldn't exist without you. The same applies to anyone who freely shares their knowledge and helps people to learn through their blog posts, newsgroup responses, and articles. The technical world is a better place because of you.

In this third edition, I feel like I'm standing on the shoulders of giants. All of the material in this book is based off of the ideas from those who came before me in the prior two editions. To those authors and editors, I thank you for laying the foundation for this edition and providing the groundwork for me to enhance with the technological improvements and changes which have occurred over the years. A thank you also to Neil Fryer for all of his efforts doing the technical editing of my work.

I owe individual thank you to Paul Hand (rAwjAw), Dave Kennedy (ReL1K), Dan Martell, and Kevin Riggins for your help with technical areas and examples used in this book. You guys really helped me out even if you didn't know it at the

time. Thank you also to Scott Bilyeu who has been the greatest sounding board and was never afraid to tell me that something didn't make sense. You may not recognize it, but you have been instrumental in helping me get this done and motivating me to keep pushing on. Drinks are on me, bro.

With all the people I've been in contact with and talked to about this book over the last year, I know I've missed some in this acknowledgment. I apologize if I missed you and I thank you from the bottom of my heart for all for the support that you have provided.

Introduction

BOOK OVERVIEW AND KEY LEARNING POINTS

Penetration testing is often considered an art as much as it is a science, but even an artist needs the right brushes to do the job well. Many commercial and open source tools exist for performing penetration testing, but it's often hard to ensure that you know what tools are available and which ones to use for a certain task. Through the next 10 chapters, we'll be exploring the plethora of open source tools that are available to you as a penetration tester, how to use them, and in which situations they apply.

Open source tools are pieces of software which are available with the source code so that the software can be modified and improved by other interested contributors. In most cases, this software comes with a license allowing for distribution of the modified software version with the requirement that the source code continue to be included with the distribution. In many cases, open source software becomes a community effort where dozens if not hundreds of people are actively contributing code and improvements to the software project. This type of project tends to result in a stronger and more valuable piece of software than what would often be developed by a single individual or small company.

While commercial tools certainly exist in the penetration testing space, they're often expensive and, in some cases, too automated to be useful for all penetration testing scenarios. There are many common situations where the open source tools that we will be talking about fill a need better and (obviously) more cost effectively than any commercial tool. The tools that we will be discussing throughout this book are all open source and available for you to use in your work as a penetration tester.

BOOK AUDIENCE

This book is primarily intended for people who either have an interest in penetration testing or perform penetration testing as a professional. The level of detail provided is intentionally set so that anyone new to the technologies used for penetration testing can understand what is being done and learn while not boring individuals who do this work on a daily basis. It is the intent of this publication that the entire audience, new or old, is able to gain valuable insights into the technologies, techniques, and open source tools used for performing penetration testing.

In addition, anyone working in the areas of database, network, system, or application administration as well as architects will be able to gain some knowledge of how penetration testers perform testing in their individual areas of expertise and

learn what to expect from a penetration test. This can help to improve the overall security of a company's applications and infrastructure and lead to a safer and better-protected environment.

Aside from penetration testers specifically, any security or audit professional should be able to use this book as a reference for tasks associated with ensuring the security of an environment. Even if you are not performing penetration testing yourself, knowing what we as penetration testers are looking at can help you to ensure that you have technology and policies in place to cover the most critical areas in your business from a security perspective.

HOW THIS BOOK IS ORGANIZED

This book is divided into a total of 10 chapters with each chapter focusing on a specific area of penetration testing. Each chapter is organized to define objectives associated with the focus area, an approach to penetration testing of that area, core technologies that you should understand when performing testing, and open source tools that can be used to perform that penetration testing. In addition, every chapter will include a real-world case study where the tools that we discussed are used in an actual scenario that a penetration tester could encounter. To add to the fun, there will also be a hands-on challenge in every chapter so that you can practice what you've learned.

While it is not necessary to read this book from beginning to end in order to gain value, it is recommended as some of the later chapters rely on knowledge gained from earlier chapters. As an example, Chapter 8 focuses on Enterprise Application Testing which requires a strong foundation in all of the areas discussed in Chapters 1−7 to be effective. If you're already an experienced penetration tester however, you may simply need information on new tools in a specific area. If that's the case, you may find more value by digging into the chapters where your interest lies and scanning through the others to pick up tips later. The following descriptions will give you a brief idea of what we'll be talking about in each chapter.

Chapter 1: Tools of the trade

In this first chapter, we'll start off by looking at some of the major bundles of tools available in the open source world for penetration testing. While all of the tools that we'll talk about throughout this book are available individually, it tends to save a lot of time and effort if you already have a package available with most or all of the tools that you may need. We'll talk about how the toolkits are built, how you can modify them or build your own, and how to use them. In addition, we'll also talk about penetration testing targets and how those can be built and used in a similar manner to help you to build a learning ground for testing the tools.

Chapter 2: Reconnaissance

The most valuable thing for any penetration tester isn't a tool, but information. By gathering information about our target, we position ourselves to be able to do our job effectively and conduct a thorough penetration test. Chapter 2 covers this area by focusing on reconnaissance and learning as much about your target as possible before you actually interact with it. This is typically a very stealthy part of penetration testing and is the first step in gathering the information that you need to move forward with your testing.

Chapter 3: Scanning and enumeration

In Chapter 3, we leverage the data gathered through our reconnaissance and expand on it. Enumeration and scanning is all about learning as much as you can about your target and ensuring that you have the details necessary to actually test the target. This includes gathering data related to what machines are available, which operating systems they're running, and which services are available on them. This phase of penetration testing is where we start to be a little more intrusive and actually "touch" our targets for the first time. Gathering the details made available through enumeration and scanning lays the foundation for our future service/system-specific penetration testing.

Chapter 4: Client-side attacks and human weaknesses

Some of the data that we gather in the reconnaissance, scanning, and enumeration phases may include information around client machines and individual people. In many penetration tests, using these is considered a valid attack vector and should be considered as a point of entry into the systems that you're attempting to compromise. In this chapter we'll be talking about social engineering and other attacks which can be used against individuals and their client workstations. We'll even go over social networking and how to use social networks as part of a penetration test.

Chapter 5: Hacking database services

For Chapter 5, we move our focus into a specific type of service, relational database management systems. Databases are a key component of every major corporation and provide an attack vector for us as penetration testers. Many databases have vulnerabilities through bugs in the software, misconfiguration, or poor security practices that we can use to either gather restricted data or compromise systems. Throughout this chapter we'll talk about different database systems, how to perform penetration testing of those systems, and which open source tools to use to do the job.

Chapter 6: Web server and web application testing

In many cases, web servers and web applications play a critical role in a corporation's infrastructure and penetration testers frequently focus on this area. This focus is typically due to the very high number of vulnerabilities that can be found in web applications and the ease in which they can be introduced. One small error in coding for a web application can fully open up the system to a penetration tester. Chapter 6 is geared toward this area and covers topics associated with the web server software itself as well as the web applications running on top of that foundation.

Chapter 7: Network devices

One of the most critical components of an enterprise is the network gear used to link it all together. In Chapter 7, we'll be talking about network devices from the perspective of penetration testing. This includes not only network devices used to provide connectivity from point A to point B, but also all of the other devices which may reside on a network. With network devices being such an important part of the overall infrastructure of a company, it's a logical focal point for penetration testing. If successfully compromised, network devices can provide data giving you access to many other targets on the network and make your job as a penetration tester very easy.

Chapter 8: Enterprise application testing

Enterprise applications are becoming one of the largest targets when performing penetration testing in corporate environments. This is due not only to their large footprint, but also to the critical data that they contain. In Chapter 8 we tie together all that we've discussed in prior chapters and use that knowledge to demonstrate how to test an enterprise application. We'll go over what defines an enterprise application, why it's important, and how it fits into a penetration testing plan.

Chapter 9: Wireless penetration testing

In all chapters prior to this, we focused on systems that we can communicate with on the network. But how do we gain access to the network itself if we don't have a direct connection? In this chapter we'll discuss wireless networks, how they work, and how they are used in corporate environments. Wireless networks can be a point of entry to the corporate network that we are attempting to test, but they can also require some testing on their own even if you do have a direct connection. We'll go over how to perform this testing for wireless networks and also discuss the expanded use of some technologies in this area such as Bluetooth and how they can be used for penetration testing as well.

Chapter 10: Building penetration test labs

As a penetration tester, you need a lab to perform some types of testing as well as perfecting your own skills. In Chapter 10, we talk about penetration test labs, what they are comprised of, and how to build them. Safety is a primary topic in this chapter as well due to the potential dangers around having an insecure penetration test lab. A number of tools associated with penetration test labs will be discussed as well as technologies such as virtualization which can help reduce the cost of building a lab. By the end of this chapter, you should be able to build your own safe penetration test lab and master the tools that have been covered throughout this book.

CONCLUSION

From a personal perspective, writing this book has really been a great experience and I hope that you enjoy reading it. Regardless of how much experience any of us have, there are always new innovations, ideas, and tools coming out on a daily basis and there is always the opportunity to learn. It is my hope that this book will provide you with a great introduction or give you the opportunity to expand your knowledge in the area of penetration testing using open source tools.

This page intentionally left blank

About the Author

Jeremy Faircloth (Security+, CCNA, MCSE, MCP+I, A+) is a Senior Principal IT Technologist for Medtronic, Inc., where he and his team architect and maintain enterprise-wide client/server and web-based technologies. He is a member of the Society for Technical Communication and frequently acts as a technical resource for other IT professionals through teaching and writing, using his expertise to help others expand their knowledge. As a systems engineer with over 20 years of real-world IT experience, he has become an expert in many areas including web development, database administration, enterprise security, network design, large enterprise applications, and project management.

Jeremy was a Contributing Author to *Security+ Study Guide & DVD Training System* (ISBN: 978-1-931836-72-2), *SSCP^{CM} Study Guide & DVD Training System* (ISBN: 978-1-931836-80-7), *Snort 2.0 Intrusion Detection* (ISBN: 978-1-931836-74-6), *Security Log Management: Identifying Patterns in the Chaos* (ISBN: 978-1-59749-042-9), *Combating Spyware in the Enterprise: Discover, Detect, and Eradicate the Internet's Greatest Threat* (ISBN: 978-1-59749-064-1), *Syngress Force Emerging Threat Analysis: From Mischief to Malicious* (ISBN: 978-1-59749-056-6), *Security+ Study Guide & DVD Training System, Second Edition* (ISBN: 978-1-59749-153-2), *Perl Scripting for Windows Security: Live Response, Forensic Analysis, and Monitoring* (ISBN: 978-1-59749-173-0), *CompTIA Security+ Certification Study Guide: Exam SY0-201, Third Edition* (ISBN: 978-1-59749-426-7), and others.

About the Technical Editor

Neil Fryer (OSCP, OSWP, CEH, GPEN, GCIH, CHFI, GCFW, MCP, SCSA) is the Technical Security Director and owner of IT Security Geeks LTD, where he and his team of consultants perform penetration testing and offer other security consultancy services to clients. He is a member of both the SANS Advisory Board and OWASP.

As a security professional with over 15 years of real-world IT experience, Neil is an expert in many areas of IT security consultancy, specializing in penetration testing and vulnerability research. He has worked for some of the world's leading financial organizations and mobile phone service providers.

Neil's true love is penetration testing, and trying to figure out how things work, breaking them, and putting them back together again. He has discovered numerous vulnerabilities on high-profile web sites and Apple's Safari web browser, and in various "Black Box" solutions.

This page intentionally left blank

CHAPTER

Tools of the trade 1

INFORMATION IN THIS CHAPTER:

- Objectives
- Approach
- Core Technologies
- Open Source Tools
- Case Study: The Tools in Action
- Hands-On Challenge

The quality of the tools that we use as penetration testers is part of what determines the quality of work that we perform. Other parts are, of course, skill, experience, and imagination. By building an excellent toolkit, we can better perform our penetration testing work and do a better, faster, and higher quality job. While the rest of this book will be focusing on individual tools and how to use them, in this chapter we will be talking about toolkits which contain a number of the tools we'll be discussing later and more.

We will also be talking about some of the technologies used to make carrying around your toolkit easier and safer. A good set of tools should always be stored in a good toolbox. In addition, we'll touch on some of the tools that you can use to build target systems for penetration testing. In Chapter 10, we'll talk about building a test lab, but here we'll talk about some of the kits that you can use within that lab.

This chapter may not be quite as interesting as the remaining chapters in this book since we will not be doing any actual penetration testing examples here. However, it is very important to have a solid foundation in the general tools available to you as a penetration tester prior to learning how to use those tools in real-world scenarios. You'll find that it saves you a lot of time later when we demonstrate using a tool if you already have a toolkit which contains it.

1.1 OBJECTIVES

Our objectives for this chapter are to learn which toolkits exist in the open source world for penetration testing, learn how those toolkits are built and how to modify

Penetration Tester's Open Source Toolkit, Third Edition. DOI: 10.1016/B978-1-59749-627-8.10001-7