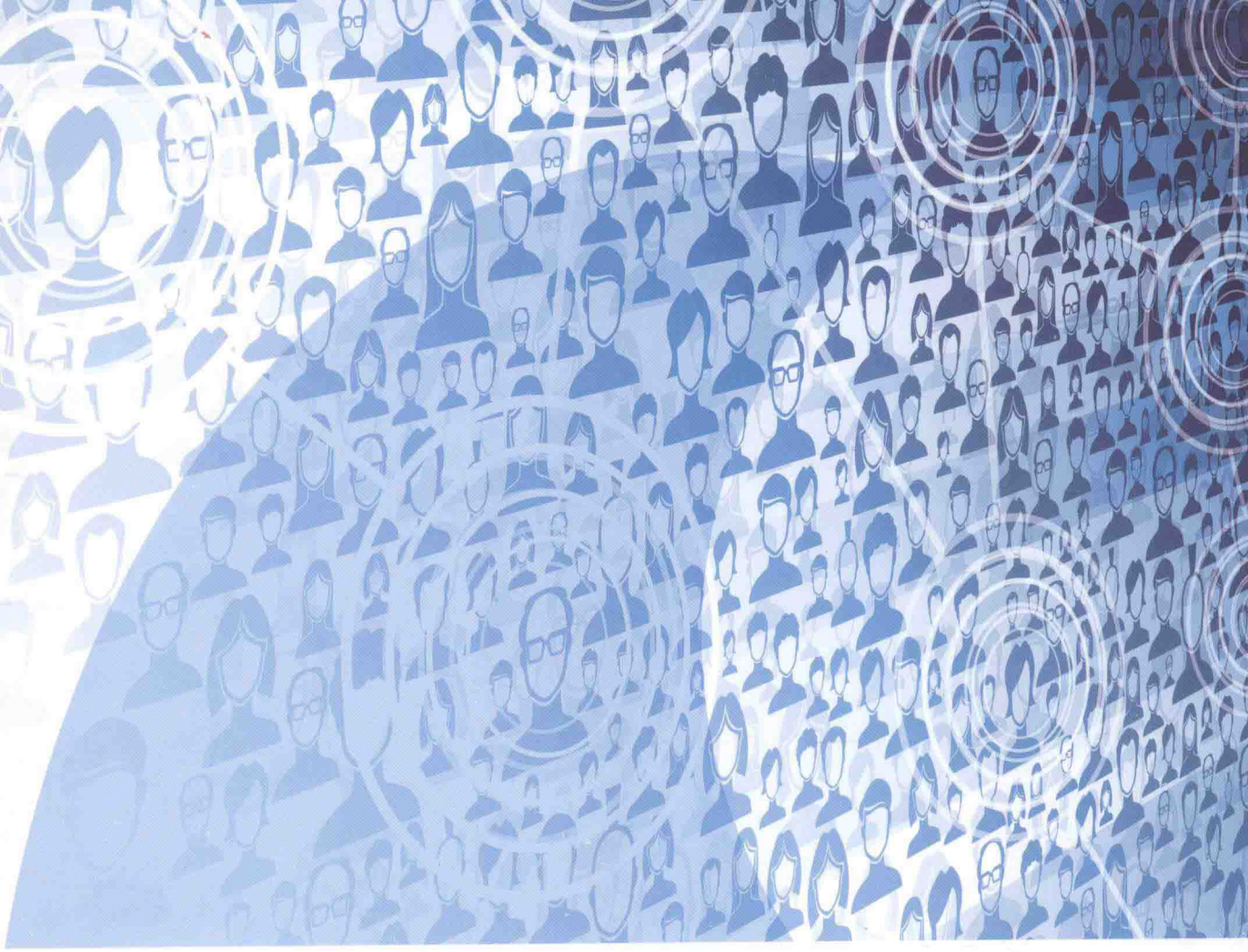


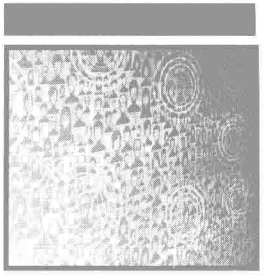
WIRESHARK®

FOR SECURITY PROFESSIONALS

Using Wireshark and the Metasploit Framework

Jessey Bullock
Jeff T. Parker

WILEY



Wireshark® for Security Professionals

Using Wireshark and the Metasploit® Framework

Jessey Bullock
Jeff T. Parker

WILEY

Wireshark® for Security Professionals: Using Wireshark and the Metasploit® Framework

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

ISBN: 978-1-118-91821-0
ISBN: 978-1-118-91823-4 (ebk)
ISBN: 978-1-118-91822-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Control Number: 2016946245

To my loving wife Heidi, my family, friends, and all those I have had the opportunity to learn from. —Jessey

To Mom. Thank you. —Jeff

Credits

Project Editor
John Sleeva

Technical Editor
Rob Shimonski

Production Editor
Athiyappan Lalith Kumar

Copy Editor
Kim Heusel

Production Manager
Katie Wisor

Manager of Content Development and Assembly
Mary Beth Wakefield

Marketing Manager
Carrie Sherrill

Professional Technology and Strategy Director
Barry Pruett

Business Manager
Amy Knies

Executive Editor
Jim Minatel

Project Coordinator, Cover
Brent Savage

Proofreader
Nancy Bell

Indexer
Nancy Guenther

Cover Designer
Wiley

Cover Image
© Jonathan Haste/iStockPhoto

About the Authors

Jessey Bullock is a security engineer with a diverse background, having worked both as a security consultant and as an internal security team member. Jessey started out supporting network administration while trying to break into the security industry, and Wireshark has always been an integral part of his tool set. His varied skill set was honed across numerous industries, such as energy and finance, even having worked for a gaming company.

Jessey's experience includes a deep understanding of offensive and application security. As a consultant, Jessey performed engagements involving everything from incident response to embedded device testing. Jessey currently focuses on application security and has a keen interest in scaling security testing while providing day to day security support for developers and performing assessments of internally developed products.

In his free time, Jessey enjoys gaming with his son, writing the occasional Python code, and playing grumpy sysadmin for his wife's restaurant business.

Jeff T. Parker is a seasoned security professional and technical writer. His 20 years of experience began with Digital Equipment Corporation, then on to Compaq and Hewlett Packard, where Jeff primarily consulted on complex enterprise environments. During the HP years, Jeff shifted his focus from systems to security. Only IT security has matched an insatiable appetite for learning and sharing.

Having done the "get as many certifications as you can" phase, Jeff is most proud of his service to clients, including UN agencies, government services, and enterprise corporations.

Jeff holds degrees in subjects far from IT, yet he only makes time to hack away at his home lab. He and his family enjoy life in Halifax, Nova Scotia, Canada.

Most excitedly, Jeff timed this project's end with a much-anticipated new project: house training a new puppy.

About the Technical Editor

Rob Shimonski (`www.shimonski.com`) is a best-selling author and editor with more than 20 years of experience developing, producing, and distributing print media in the form of books, magazines, and periodicals, and more than 25 years working in the Information Technology field. To date, Rob has successfully helped create, as both an author and an editor, more than 100 books that are currently in circulation. Rob has an extremely diverse background in the print media industry, filling roles such as author, co-author, technical editor, copy editor, and developmental editor. Rob has worked for countless companies, including CompTIA, Cisco, Microsoft, Wiley, McGraw Hill Education, Pearson, the National Security Agency, and the US military.

As a Wireshark guru, Rob's experience goes back to the beginning of the application's existence. Having worked with Ethereal and various other packet capturing tools, Rob has been at the forefront of watching Wireshark evolve into the outstanding tool it is today. Rob has also captured this evolution in various written works, including *Sniffer Pro: Network Optimization and Troubleshooting Handbook* (Syngress, 2002) and *The Wireshark Field Guide: Analyzing and Troubleshooting Network Traffic* (Syngress, 2013). Rob has also worked with INE.com to create a practitioner and advanced practitioner video series detailing the usage and how to work with Wireshark in 2015. In 2016, Rob focused his energies on helping other authors develop their works to ensure technical accuracy in advanced topics within the Wireshark toolset. Rob is also certified as both a Wireshark Certified Network Analyst (WCNA) and a Sniffer Pro SCP.

Acknowledgments

This book owes a big thank you to the awesome developers of the Wireshark suite, as well as the developers of Metasploit, Lua, Docker, Python, and all the other open-source developers who make amazing technology accessible. Thanks also to the people at Wiley for putting up with me, especially John Sleeva and Jim Minatel, and to Rob Shimonski, the fantastic technical editor who helped keep the book correct and useful. Special thanks go to my co-author Jeff Parker for taking on the challenge of writing this book. He was a blast to work with and is owed immense credit for helping make this book possible.

I would also like to thank Jan Kadijk, John Heasman, Jeremy Powell, Tony Cargile, Adam Matthews, Shaun Jones, and Connor Kennedy for contributing ideas and support.

—Jessey

Kudos to the Wiley team, including Jim Minatel, John Sleeva, and Kim Heusel, for their dedication to carry this book to the finish line. Big thanks to Rob Shimonski, the technical editor, who performed with great patience to ensure we left no gaps or confusion.

To Jessey, the book's visionary and the W4SP Lab guru, I thank you for being ever gracious and collaborative. All your effort concludes with a book and online resources that we can both be proud of.

To Carole Jelen, my literary agent in sunny southern California, all opportunities start with you. You are an endless provider of growth and have my deep gratitude. Thanks, Carole!

The biggest thanks go to my wife and my best friend. I'm grateful for her patience and support. To our two kids, Dad is back and ready to play (and research for the next book—wink, wink).

—Jeff

Introduction

Welcome to *Wireshark for Security Professionals*. This was an exciting book for us to write. A combined effort of a few people with varied backgrounds—spanning information security, software development, and online virtual lab development and teaching—this book should appeal and relate to many people.

Wireshark is *the* tool for capturing and analyzing network traffic. Originally named Ethereal but changed in 2006, Wireshark is well established and respected among your peers. But you already knew that, or why would you invest your time and money in this book? What you're really here for is to delve into how Wireshark makes your job easier and your skills more effective.

Overview of the Book and Technology

This book hopes to meet three goals:

- Broaden the information security professional's skillset through Wireshark.
- Provide learning resources, including labs and exercises, to apply what you learn.
- Demonstrate how Wireshark helps with real-life scenarios through Lua scripting.

The book isn't only for reading; it's for doing. Any Wireshark book can show how wonderful Wireshark can be, but this book also gives you opportunities to practice the craft, hone your skills, and master the features Wireshark offers.

These opportunities come in a few forms. First, to apply what's in the text, you will practice in labs. You build the lab environment early on the book and put it to use throughout the chapters that follow. The second opportunity

for practice is at the end of each chapter, save the last Lua scripting chapter. The end-of-chapter exercises largely build on the labs to challenge you again, but with far less hand-holding. Between the labs and exercises, your time spent with Wireshark ensures time spent reading is not forgotten.

The lab environment was created using containerization technology, resulting in a fairly lightweight virtual environment to be installed and run on your own system. The whole environment was designed specifically for you, the book reader, to practice the book's content. These labs were developed and are maintained by one of the authors, Jessey Bullock. The source code for the labs is available online. See Chapter 2 for specifics.

In short, this book is a hands-on, practice-oriented Wireshark guide created for you, the information security professional. The exercises will help you to keep you advancing your Wireshark expertise long after the last page.

How This Book Is Organized

The book is structured on the assumption that readers will start from the beginning and then work through the main content. The initial three chapters not only introduce the title application Wireshark but also the technology to be used for the labs, along with the basic concepts required of the reader. Readers already familiar with Wireshark should still work through the lab setup chapter, since future chapters depend on the work being done. These first three chapters are necessary to cover first, before putting the following chapters to use.

The majority of the book that follows is structured to discuss Wireshark in the context of information security. Whether capturing, analyzing, or confirming attacks, the book's main content and its labs are designed to most benefit information security professionals.

The final chapter is built around the scripting language Lua. Lua greatly increases Wireshark's flexability as an already powerful network analyzer. Initially, the Lua scripts were scattered thoughout chapters, but they were later combined into a single chapter all their own. It was also appreciated that not all readers are coders, so Lua scripts are better served through one go-to resource.

Here's a summary of the book's contents:

Chapter 1, "Introducing Wireshark," is best for the professional with little to no experience with Wireshark. The main goal is to help you avoid being overwhelmed, introduce the interface, and show how Wireshark can be your friend.

Chapter 2, "Setting Up the Lab," is not to be skipped. Starting with setting up a virtualized machine, this chapter then sets up the W4SP Lab, which you will use several times in upcoming chapters.

Chapter 3, "The Fundamentals," covers basic concepts and is divided into three parts: networking, information security, and packet analysis. The book assumes most readers might be familiar with at least one or two areas, but the chapter makes no assumptions.

Chapter 4, "Capturing Packets," discusses network captures, or the recording of network packets. We take a deep dive into how Wireshark captures, manipulates capture files, and interprets the packets. There's also a discussion around working with the variety of devices you encounter on a network.

Chapter 5, "Diagnosing Attacks," makes good use of the W4SP Lab, re-creating various attacks commonly seen in the real world. Man in the middle attacks, spoofing various services, denial of service attacks and more are all discussed.

Chapter 6, "Offensive Wireshark," also covers malicous traffic, but from the hacker's perspective. Wireshark and the W4SP Lab are again relied on to launch, debug, and understand exploits.

Chapter 7, "Decrypting TLS, Capturing USB, Keyloggers, and Network Graphing," is a mash-up of more activities as we leverage Wireshark. From decrypting SSL/TLS traffic to capturing USB traffic across multiple platforms, this chapter promises to demonstrate something you can use wherever you work or play.

Chapter 8, "Scripting with Lua," contains about 95% of the book's script content. It starts simple with scripting concepts and Lua setup, whether you're working on Windows or Linux. Scripts start with "Hello, World" but lead to packet counting and far more complex topics. Your scripts will both enhance the Wireshark graphic interface and run from the command line.

Who Should Read This Book

To claim this book is for security professionals might be specific enough to the general IT crowd. However, to most information security professionals, it's still too broad a category. Most of us specialize in some way or another, and identify ourselves by our role or current passion. Some examples include firewall administrator, network security engineer, malware analyst, and incident responder.

Wireshark is not limited to just one or two of those roles. The need for Wireshark can be found in roles such as penetration tester or ethical hacker—roles defined by being proactive and engaging. Additional roles like forensics analyst, vulnerability tester, and developer also benefit from being familiar with Wireshark. We'll show this through examples in the book.

Regarding expectations on the reader, the book makes no assumptions. Information security specializations vary enough so that someone with 15 years of experience in one field is likely a novice in other fields. Wireshark offers value for anyone in those fields, but it does expect a basic understanding of networking, security and how protocols work. Chapter 3 ensures we're all on the same page.

Any reader must be technically savy enough to install software or understand systems are networked. And since the book targets security professionals, we presume a fundamental level for information security. Still, as far as

"fundamentals" go, Chapter 3 acts as a refresher for what's necessary around networking, information security, and packet and protocol analysis.

Further in the book, Wireshark is used in the context of various roles, but there's no experience requirement for grasping the content or making use of the labs. For example, the tools used in Chapter 6, "Offensive Wireshark" might be already familiar to the penetration tester, but the chapter assumes zero experience when instructing setup.

To sum up, we understand there is a wide spectrum of possible roles and experience levels. You might be employed in one of these roles and want to use Wireshark more. Or you might be getting ready to take on one of these roles, and recognize Wireshark as essential tool to use. In either case, this book is for you.

Tools You Will Need

The one tool required for this book is a system. Your system does not need to be especially powerful; at the most a few years old would be best. Your system will be first used in Chapter 2, "Setting Up the Lab." You first install and set up a virtualized machine. Then upon that virtual machine you will set up the labs.

Of course, this book can benefit those without a system, but a system is needed to perform the labs referenced throughout the book.

What's on the Website

The primary website needed for this book is the GitHub repository for the W4SP Lab code. The GitHub repo and its contents are explained further in Chapter 2, "Setting Up the Lab," where you first download and build the virtual lab environment. Then the Lab files are installed onto your virtual machine.

Other websites are cited throughout the book, mostly as pointers for additional resources. For example, some sites hold hundreds of network capture files that are available for analysis.

Summary

This is where the authors are at the edge of our seats, hoping you will leap into and enjoy the book, its materials, and the labs. A lot of thought and effort went into this book. Our only desire was to create a resource that inspired more people to have a deeper appreciation of Wireshark. Being information security professionals ourselves, we crafted this book for our peers.

Contents