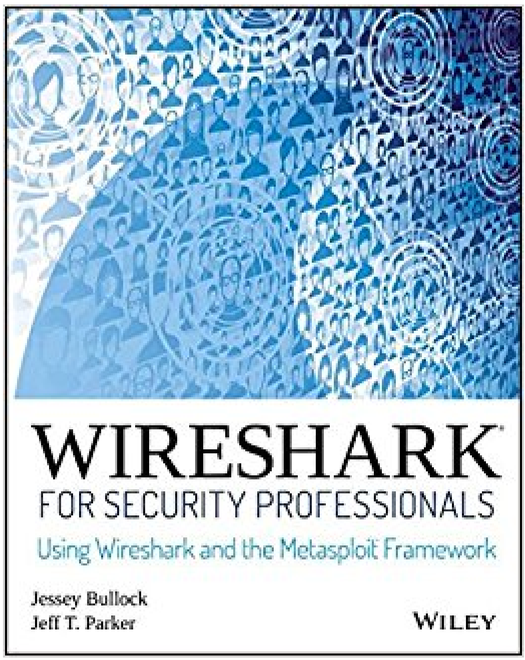
Wireshark For Security Professionals: Using Wireshark And The Metasploit Framework


WIRESHARK
FOR SECURITY PROFESSIONALS
Using Wireshark and the Metasploit Framework
Jessey Bullock
Jeff T. Parker
WILEY

Synopsis

Master Wireshark to solve real-world security problemsÂ If you donâ ™t already use Wireshark for a wide range of information security tasks, you will after this book. Mature and powerful, Wireshark is commonly used to find root cause of challenging network issues. This book extends that power to information security professionals, complete with a downloadable, virtual lab environment. Wireshark for Security Professionals covers both offensive and defensive concepts that can be applied to essentially any InfoSec role. Whether into network security, malware analysis, intrusion detection, or penetration testing, this book demonstrates Wireshark through relevant and useful examples. Master Wireshark through both lab scenarios and exercises. Early in the book, a virtual lab environment is provided for the purpose of getting hands-on experience with Wireshark. Wireshark is combined with two popular platforms: Kali, the security-focused Linux distribution, and the Metasploit Framework, the open-source framework for security testing. Lab-based virtual systems generate network traffic for analysis, investigation and demonstration. In addition to following along with the labs you will be challenged with end-of-chapter exercises to expand on covered material. Lastly, this book explores Wireshark with Lua, the light-weight programming language. Lua allows you to extend and customize Wiresharkâ ™s features for your needs as a security professional. Lua source code is available both in the book and online. Lua code and lab source code are available online through GitHub, which the book also introduces. The bookâ ™s final two chapters greatly draw on Lua and TShark, the command-line interface of Wireshark. By the end of the book you will gain the following: Master the basics of Wireshark Explore the virtual w4sp-lab environment that mimics a real-world network Gain experience using the Debian-based Kali OS among other systems Understand the technical details behind network attacks Execute exploitation and grasp offensive and defensive activities, exploring them through Wireshark Employ Lua to extend Wireshark features and create useful scripts To sum up, the book content, labs and online material, coupled with many referenced sources of PCAP traces, together present a dynamic and robust manual for information security professionals seeking to leverage Wireshark. Â

Book Information

Paperback: 288 pages

Publisher: Wiley; 1 edition (March 20, 2017)

Language: English

ISBN-10: 1118918215

ISBN-13: 978-1118918210

Product Dimensions: 7.2 x 0.7 x 9 inches

Shipping Weight: 1 pounds (View shipping rates and policies)

Average Customer Review: 4.8 out of 5 stars   5 customer reviews

Best Sellers Rank: #47,174 in Books (See Top 100 in Books)   #23 inÂ Books > Computers & Technology > Security & Encryption > Encryption   #23 inÂ Books > Computers & Technology > Security & Encryption > Cryptography   #53 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security

Customer Reviews

An essential guide to network security and the feature-packed Wireshark toolset Open source protocol analyzer Wireshark is the de facto analysis tool across many fields, including the security field. Wireshark provides a powerful feature set that allows you to inspect your network at a microscopic level. The diverse features and support for numerous protocols make Wireshark an invaluable security tool, but also difficult or intimidating for newcomers to learn. Wireshark for Security Professionals is the answer, helping you to leverage Wireshark and related tools such as the command line TShark application quickly and effectively. Coverage includes a complete primer on Metasploit, the powerful offensive tool, as well as Lua, the popular scripting language. This highly practical guide gives you the insight you need to successfully apply what you&#39;ve learned in the real world. Examples show you how Wireshark is used in an actual network with the provided Docker virtual environment, and basic networking and security principles are explained in detail to help you understand the why along with the how. Using the Kali Linux penetration testing distribution in combination with the virtual lab and provided network captures, you can follow along with the numerous examples or even start practicing right away in a safe network environment. The hands-on experience is made even more valuable by the emphasis on cohesive application, helping you exploit and expand Wireshark&#39;s full functionality by extending Wireshark or integrating it with other security tools. With coverage of both offensive and defensive security tools and techniques, Wireshark for Security Professionals shows you how to secure any network as you learn to: Understand the basics of Wireshark and the related toolset as well as the Metasploit Framework Explore the Lua scripting language and how it can be used to extend Wireshark Perform common offensive and defensive security research tasks with Wireshark Gain hands-on experience in a Docker virtual lab environment that replicates real-world enterprise networks Capture packets using advanced MitM techniques Customize the provided source code to expand your toolset

JESSEY BULLOCK is a Senior Application Security Engineer with a game company. Having previously worked at both NGS and iSEC Partners as a consultant, he has a deep understanding of application security and development, operating systems internals, and networking protocols. Jessey has experience working across multiple industry sectors, including health care, education, and security. Jessey holds multiple security certifications, including CISSP, CCNA, CWNA, GCFE, CompTIA Security+, CompTIA A+, OSCP, GPEN, CEH, and GXPN.Â JEFF T. PARKER is a seasoned IT security consultant with a career spanning 3 countries and as many Fortune 1OO companies. Now in Halifax, Canada, Jeff enjoys life most with his two young children, hacking professionally while they&apos;re in school.

I’m still making my way through the book, but here are my initial impressions:There is A LOT of hand holding throughout the book. I, personally, like this but it may turn some people off or just have them skip the extra explanations. This is definitely a book for beginners and if you already have some experience with Wireshark or Kali you may find the information presented as a nice refresher or prefer to skip to the chapters that are relevant to you.This book does not solely focus on Wireshark, but also on methodologies used by security professionals. It implements MSF and other tools one would use on a regular basis. I’m looking forward to continue with the labs and explanations throughout the rest of the book.If you’re new to the field or are looking to expand into new areas, I would highly recommend this book. If you have already been around the block for some time, you may already know most of the information presented but may benefit by some of the more updated information the authors bring in.

Everyone’s favorite

The book and the lab environment for this are great aids to help people learn what exploitation looks like.

This a very well written book and taught more than I anticipated. He also guides people to set up a Kali Linux VM and delved into Dockers and containers which was an added bonus that I was not expecting. He did a very thorough job on the actual subject of Wireshark with lots of useful insights.

Excellent reference.

Download to continue reading...

Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Practical Packet Analysis, 3E: Using Wireshark to Solve Real-World Network Problems Programming Entity Framework: DbContext: Querying, Changing, and Validating Your Data with Entity Framework FrameWork for the Lower Back:Â A 6-Step Plan for a Healthy Lower Back (FrameWork Active for Life) Ict Framework Solutions: Year 8 (Ict Framework Solutions S.) Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security: Volume 28 NATO Science for Peace and Security Series - D: ... D: Information and Communication Security) Nuclear Safeguards, Security and Nonproliferation: Achieving Security with Technology and Policy (Butterworth-Heinemann Homeland Security) Security Camera For Home: Learn Everything About Wireless Security Camera System, Security Camera Installation and More Fundamentals Of Information Systems Security (Information Systems Security & Assurance) - Standalone book (Jones & Bartlett Learning Information Systems Security & Assurance) The Growth Gears: Using A Market-Based Framework To Drive Business Success Phaser.js Game Design Workbook: Game development guide using Phaser JavaScript Game Framework The Handbook for Enhancing Professional Practice: Using the Framework for Teaching in Your School Preparing Educators to Engage Families: Case Studies Using an Ecological Systems Framework Law, Liability, and Ethics for Medical Office Professionals (Law, Liability, and Ethics Fior Medical Office Professionals) Ethical and Legal Issues for Imaging Professionals, 2e (Towsley-Cook, Ethical and Legal Issues for Imaging Professionals) Long-Term Care for Activity Professionals, Social Services Professionals, and Recreational Therapists Sixth Edition The Low Vision Handbook for Eyecare Professionals (Basic Bookshelf for Eyecare Professionals) Kickboxing Fitness: A Guide For Fitness Professionals From The American Council On Exercise (Guides for Fitness Professionals) (Ace’s Group Fitness Specialty)

Contact Us

DMCA

Privacy

FAQ & Help