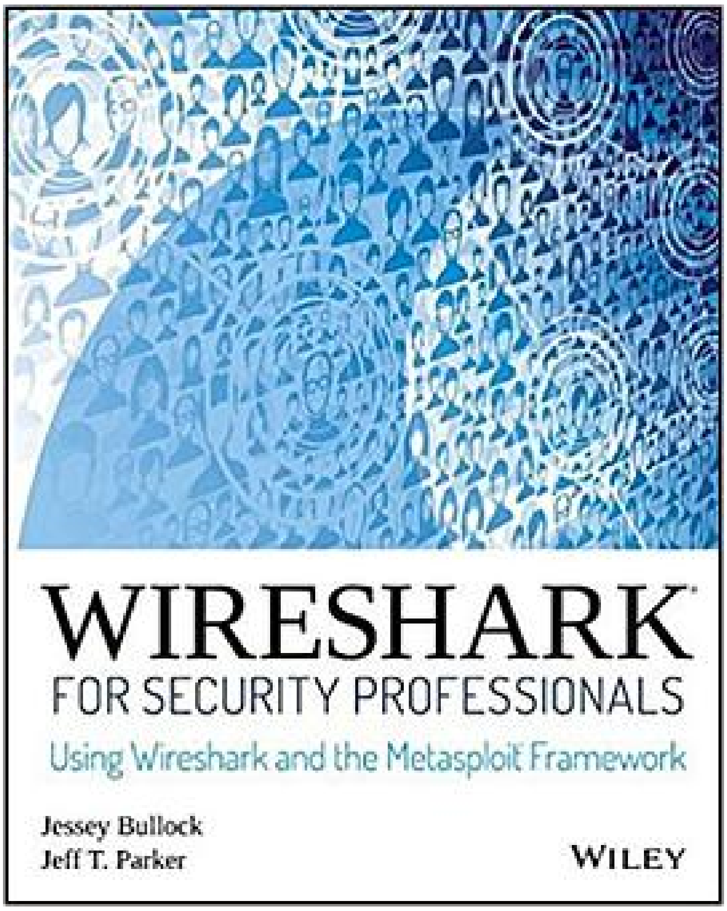
Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework



[Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework_下载链接1_]

著者:Jessey Bullock

出版者:Wiley

出版时间:2017-3-20

装帧:Paperback

isbn:9781118918210

If you don’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 Wireshark’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 book’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.

作者介绍:

From the Back Cover

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'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'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

Read more

About the Author

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.JEFF T. PARKER is a seasoned IT security consultant with a career spanning 3 countries and as many Fortune 100 companies. Now in Halifax, Canada, Jeff enjoys life most with his two young children, hacking professionally while they're in school.

Read more

目录:

Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework_下载链接1_

标签

wireshark

渗透测试

评论

Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework_下载链接1_

书评

Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework_下载链接1_