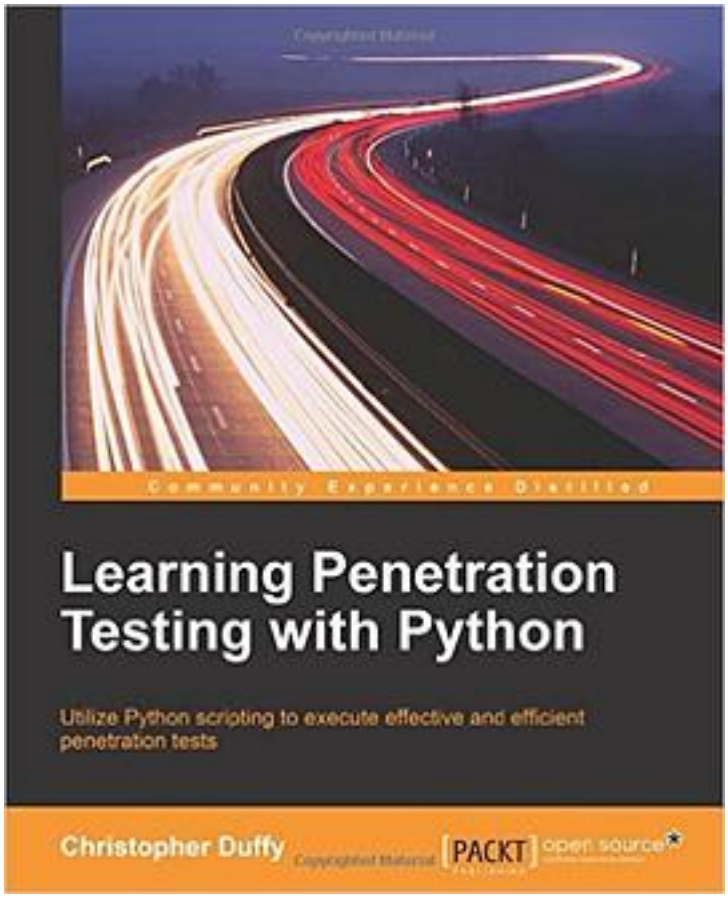
Learning Penetration Testing with Python



Learning Penetration Testing with Python_下载链接1_

著者:Christopher Duffy

出版者:Packt Publishing

出版时间:2015-11-2

装帧:Paperback

isbn:9781785282324

Utilize Python scripting to execute effective and efficient penetration tests

About This Book

Understand how and where Python scripts meet the need for penetration testingFamiliarise yourself with the process of highlighting a specific methodology to exploit an environment to fetch critical dataDevelop your Python and penetration testing skills with real-world examples

Who This Book Is For

If you are a security professional or researcher, with knowledge of different operating systems and a conceptual idea of penetration testing, and you would like to grow your knowledge in Python, then this book is ideal for you.

What You Will Learn

Familiarise yourself with the generation of Metasploit resource filesUse the Metasploit Remote Procedure Call (MSFRPC) to automate exploit generation and executionUse Python's Scrapy, network, socket, office, Nmap libraries, and custom modulesParse Microsoft Office spreadsheets and eXtensible Markup Language (XML) data filesWrite buffer overflows and reverse Metasploit modules to expand capabilitiesExploit Remote File Inclusion (RFI) to gain administrative access to systems with Python and other scripting languagesCrack an organization's Internet perimeterChain exploits to gain deeper access to an organization's resourcesInteract with web services with Python

In Detail

Python is a powerful new-age scripting platform that allows you to build exploits, evaluate services, automate, and link solutions with ease. Python is a multi-paradigm programming language well suited to both object-oriented application development as well as functional design patterns. Because of the power and flexibility offered by it, Python has become one of the most popular languages used for penetration testing.

This book highlights how you can evaluate an organization methodically and realistically. Specific tradecraft and techniques are covered that show you exactly when and where industry tools can and should be used and when Python fits a need that proprietary and open source solutions do not.

Initial methodology, and Python fundamentals are established and then built on. Specific examples are created with vulnerable system images, which are available to the community to test scripts, techniques, and exploits. This book walks you through real-world penetration testing challenges and how Python can help.

From start to finish, the book takes you through how to create Python scripts that meet relative needs that can be adapted to particular situations. As chapters progress, the script examples explain new concepts to enhance your foundational knowledge, culminating with you being able to build multi-threaded security tools, link security tools together, automate reports, create custom exploits, and expand Metasploit modules.

Style and approach

This book is a practical guide that will help you become better penetration testers and/or Python security tool developers. Each chapter builds on concepts and tradecraft using detailed examples in test environments that you can simulate.

作者介绍:

About the Author

Christopher Duffy

Christopher Duffy currently leads cybersecurity and penetration testing engagements globally. He has a specialization in advanced technical testing, including penetration testing and security assessment done to evaluate an organization's security strategy from a malicious actor's perspective. He has worked a lot with both network and system engineering teams to evaluate critical system data flows, and identified areas where controls can be put in place to prevent a breach of sensitive or critical data. His work with multiple organizations has been key to protecting resources based on the information they have held, which has helped reduce risks while maintaining resilient and cost-effective security postures. Chris has over 12 years of experience in the information technology and security areas, including security consultation, with a focus on business risk. He has helped build advanced attack and penetration teams. The work that his teams have done has encompassed everything from threat modeling and penetration tests to firewall reviews and FedRAMP readiness assessments. Chris has led, managed, and executed over 400 engagements for Fortune 500 companies, U.S. government entities, medical providers and payers, educational institutes, financial services, research organizations, and cloud providers. For almost a decade prior to private sector work, Chris was a cyber warfare specialist, senior systems engineer, and network infrastructure supervisor for the United States Air Force (USAF). He has been honored with numerous technical and leadership awards. Some of these include the (ISC)2 Information Security Leadership Award (ISLA) for the information security practitioner category in 2013, the noncommissioned officer of the year (both at the base and wing levels) in 2011, and the top technician within the cyber transport career field for the United States Air Force (USAF) Intelligence Surveillance and Reconnaissance Agency. He is a distinguished graduate of USAF network warfare training and has publications to his credit in SANS Reading Room, Hackin9 magazine, eForensics magazine and PenTest magazine. He holds 23 certifications, a degree in computer science, and a master's degree in information security and assurance.

目录:

标签

网络安全

python

评论

Learning Penetration Testing with Python_下载链接1_

书评

Learning Penetration Testing with Python_下载链接1_