Community Experience Distilled

Kali Linux – Assuring Security by Penetration Testing

Master the art of penetration testing with Kali Linux

Lee Allen
Tedi Heriyanto
Shakeel Ali

[PACKT] PUBLISHING open source* community experience distilled

Kali Linux – Assuring Security by Penetration Testing

Master the art of penetration testing with Kali Linux

Lee Allen

Tedi Heriyanto

Shakeel Ali

[PACKT] PUBLISHING

open source
community experience distilled

BIRMINGHAM - MUMBAI

Kali Linux – Assuring Security by Penetration Testing

First published: April 2011

Second Edition: April 2014

Production Reference: 2310314

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-84951-948-9

www.packtpub.com

Cover Image by Riady Santoso (dzign.art@gmail.com)

Credits

Authors

Lee Allen

Tedi Heriyanto

Shakeel Ali

Reviewers

Alex Gkiouros

Neil Jones

Acquisition Editors

Harsha Bharwani

Usha Iyer

Rubal Kaur

Content Development Editor

Sweny M. Sukumaran

Technical Editors

Mrunal Chavan

Pankaj Kadam

Gaurav Thingalaya

Copy Editors

Janbal Dharmaraj

Dipti Kapadia

Sayanee Mukherjee

Stuti Srivastava

Project Coordinator

Sanchita Mandal

Proofreaders

Simran Bhogal

Maria Gould

Paul Hindle

Indexer

Hemangini Bari

Graphics

Yuvraj Mannari

Abhinash Sahu

Production Coordinator

Alwin Roy

Cover Work

Alwin Roy

About the Authors

Lee Allen is currently working as a security architect at a prominent university. Throughout the years, he has continued his attempts to remain up to date with the latest and greatest developments in the security industry and the security community. He has several industry certifications including the OSWP and has been working in the IT industry for over 15 years.

Lee Allen is the author of *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Packt Publishing*.

I would like to thank my wife, Kellie, and our children for allowing me to give the time I needed to work on this book. I would also like to thank my grandparents, Raymond and Ruth Johnson, and my wife's parents, George and Helen Slocum. I appreciate your encouragement and support throughout the years.

Tedi Heriyanto currently works as a principal consultant in an Indonesian information security company. In his current role, he has been engaged with various penetration testing assignments in Indonesia and other countries. In his previous role, he was engaged with several well-known business institutions across Indonesia and overseas. Tedi has an excellent track record in designing secure network architecture, deploying and managing enterprise-wide security systems, developing information security policies and procedures, performing information security audits and assessments, and providing information security awareness training. In his spare time, he manages to research, learn, and participate in the Indonesian Security Community activities and has a blog `http://theriyanto.wordpress.com`. He shares his knowledge in the security field by writing several information security books.

I would like to thank my family for supporting me during the whole book-writing process. I would also like to thank my boss for trusting, helping, and supporting me in my work. I would like to thank my colleagues and customers for the great learning environment. Thanks to the great people at Packt Publishing: Rubal Kaur, Sweny Sukumaran, Joel Goveya, Usha Iyer, and Abhijit Suvarna, whose comments, feedbacks, and support made this book development project successful. Thanks to the technical reviewers, Alex Gkiouros and Neil Jones, who have provided their expertise, time, efforts, and experiences in reviewing the book's content. Last but not least, I would like to give my biggest thanks to the co-authors, Lee Allen and Shakeel Ali, whose technical knowledge, motivation, ideas, challenges, questions, and suggestions made this book-writing process a wonderful journey.

Finally, I would like to thank you for buying this book. I hope you enjoy reading the book as I enjoyed writing it. I wish you good luck in your information security endeavor.

Shakeel Ali is a Security and Risk Management consultant at Fortune 500. Previously, he was the key founder of Cipher Storm Ltd., UK. His expertise in the security industry markedly exceeds the standard number of security assessments, audits, compliance, governance, and forensic projects that he carries out in day-to-day operations. He has also served as a Chief Security Officer at CSS Providers SAL. As a senior security evangelist and having spent endless nights without taking a nap, he provides constant security support to various businesses, educational organizations, and government institutions globally. He is an active, independent researcher who writes various articles and whitepapers and manages a blog at `Ethical-Hacker.net`. Also, he regularly participates in BugCon Security Conferences held in Mexico, to highlight the best-of-breed cyber security threats and their solutions from practically driven countermeasures.

I would like to thank all my friends, reviewers, and colleagues who were cordially involved in this book project. Special thanks to the entire Packt Publishing team and their technical editors and reviewers, who have given invaluable comments, suggestions, feedbacks, and support to make this project successful. I also want to thank my co-authors, Lee Allen and Tedi Heriyanto, whose continual dedication, contributions, ideas, and technical discussions led to the production of such a useful product you see today. Last but not least, thanks to my pals from past and present with whom the sudden discovery never ends and their vigilant eyes that turn the IT industry into a secure and stable environment.

About the Reviewers

Alex Gkiouros is currently an independent IT professional who's been assigned various projects around Greece and has been working in the IT industry since 2006. He holds two entry-level ISACA certifications, and he's studying for his CCNP. He is so passionate about what he does that he spends an inordinate amount of time in the network security area, especially pentesting with Kali Linux or Backtrack. His personal website or blog can be found at `http://www.voovode.net/`.

Neil Jones is a security consultant, working for a global security company based in the UK. His goal was to work in the security industry from a young age and now he has achieved that goal, while gaining multiple industry-recognized security certifications along the way.

He eats, sleeps, and breathes security and is actively involved in security research to advance his knowledge and to develop new open source tools in order to benefit the security community.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit `www.PacktPub.com` for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

`http://PacktLib.PacktPub.com`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read and search across Packt's entire library of books.

Why Subscribe?

- Fully searchable across every book published by Packt
- Copy and paste, print and bookmark content
- On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Disclaimer

The content within this book is for educational purposes only. It is designed to help users test their own system against information security threats and protect their IT infrastructure from similar attacks. Packt Publishing and the authors of this book take no responsibility for actions resulting from the inappropriate usage of learning materials contained within this book.

I would like to dedicate this book to my loving family for their kind support throughout the years, especially to my niece, Jennifer, and nephews, Adan and Jason, whose smiles are an inspiration and encouragement in my life; to my brilliant teachers, the ones who turned an ordinary child into this superior, excellent, and extraordinary individual; and to all my friends and colleagues, Amreeta Poran, Li Xiang, Fazza3, Sheikha Maitha, Touraj, Armin, Mada, Rafael, Khaldoun, Niel, Oscar, Serhat, Kenan, Michael, Ursina, Nic, Nicole, Andreina, Amin, Pedro, Juzer, Ronak, Cornel, Marco, Selin, Jenna, Yvonne, Cynthia, May, Corinne, Stefanie, Rio, Jannik, Carmen, Gul Naz, Stella, Patricia, Mikka, Julian, Snow, Matt, Sukhi, Tristan, Srajna, Padmanabhan, Radhika, Gaurav, Eljean Desamparado, Akeela, Naveed, Asif, Salman, and all those whom I have forgotten to mention here.

- Shakeel Ali

I would like to dedicate this book to God for the amazing gifts that have been given to me; to my beloved family for their support; to my wonderful teachers for being so patient in teaching me; to my best friends and colleagues for helping me out during the years; to my excellent clients for trusting in me and giving me the chance to work with you; to you, the reader, for buying this book and e-book.

- Tedi Heriyanto

I would like to dedicate this book to those of you that have provided the security industry with the tools that empower us, the research that enlightens us, and the friendships that sustain us.

- Lee Allen

Table of Contents

Preface

Kali Linux is a penetration testing and security auditing platform with advanced tools to identify, detect, and exploit any vulnerabilities uncovered in the target network environment. Applying an appropriate testing methodology equipped with well-defined business objectives and a scheduled test plan will result in the robust penetration testing of your network.

Kali Linux – Assuring Security by Penetration Testing is a fully focused, structured book that provides guidance on developing practical penetration testing skills by demonstrating the cutting-edge hacker tools and techniques in a coherent step-by-step strategy. It offers all the essential lab preparation and testing procedures to reflect real-world attack scenarios from your business perspective in today's digital age.

This book reveals the industry's best approach for logical and systematic penetration testing process.

This book starts with lab preparation and testing procedures, explaining the basic installation and configuration setup, discussing different types of penetration testing, uncovering open security testing methodologies, and proposing the Kali Linux specific testing process. We shall discuss a number of security assessment tools necessary to conduct penetration testing in their respective categories (target scoping, information gathering, discovery, enumeration, vulnerability mapping, social engineering, exploitation, privilege escalation, maintaining access, and reporting), following the formal testing methodology. Each of these tools is illustrated with real-world examples to highlight their practical usage and proven configuration techniques. We have also provided extra weaponry treasures and key resources that may be crucial to any professional penetration testers.

This book will serve as a single professional, practical, and expert guide to develop necessary penetration testing skills from scratch. You will be trained to make the best use of Kali Linux either in a real-world environment or in an experimental test bed.

What this book covers

Chapter 1, *Beginning with Kali Linux*, introduces you to Kali Linux, a Live DVD Linux distribution specially developed to help in the penetration testing process. You will learn a brief history of Kali Linux and several categories of tools that Kali Linux has. Next, you will also learn how to get, use, configure, and update Kali Linux as well as how to configure several important network services (HTTP, MySQL, and SSH) in Kali Linux. You will also learn how to install and configure a vulnerable virtual machine image for your testing environment and several ways that can be used to install additional tools in Kali Linux.

Chapter 2, *Penetration Testing Methodology*, discusses the basic concepts, rules, practices, methods, and procedures that constitute a defined process for a penetration testing program. You will learn about making a clear distinction between two well-known types of penetration testing, black box and white box. The differences between vulnerability assessment and penetration testing will also be analyzed. You will also learn about several security testing methodologies and their core business functions, features, and benefits. These include OSSTMM, ISSAF, OWASP, and WASC-TC. Thereafter, you will learn about a general penetration Kali Linux testing process incorporated with 10 consecutive steps to conduct a penetration testing assignment from an ethical standpoint.

Chapter 3, *Target Scoping*, covers a scope process to provide necessary guidelines on normalizing the test requirements. A scope process will introduce and describe each factor that builds a practical roadmap towards test execution. This process integrates several key elements, such as gathering client requirements, preparing a test plan, profiling test boundaries, defining business objectives, and project management and scheduling. You will learn to acquire and manage the information about the target's test environment.

Chapter 4, *Information Gathering*, introduces you to the information gathering phase. You will learn how to use public resources to collect information about the target environment. Next, you learn how to analyze DNS information and collect network routing information. Finally, you will learn how to utilize search engines to get information of the target domain, e-mail addresses, and document metadata from the target environment.

Chapter 5, *Target Discovery*, introduces you to the target discovery process. You will learn the purpose of target discovery and the tools that can be used to identify target machines. At the end of this chapter, you will also learn about the tools that can be used to perform OS fingerprinting on the target machines.

Chapter 6, *Enumerating Target*, introduces you to target enumeration and its purpose. You will learn a brief theory on port scanning and several tools that can be used to do port scanning. You will also learn about various options available to be used by the Nmap port scanner tool. Also, you will learn about how to find SMB, SNMP, and VPN available in the target machine in the last part of the chapter.

Chapter 7, *Vulnerability Mapping*, discusses two generic types of vulnerabilities: local and remote. You will get insights on vulnerability taxonomy, pointing to industry standards that can be used to classify any vulnerability according to its unifying commonality pattern. Additionally, you will learn a number of security tools that can assist you in finding and analyzing the security vulnerabilities present in a target environment. These include OpenVAS, Cisco, Fuzzing, SMB, SNMP, and web application analysis tools.

Chapter 8, *Social Engineering*, covers some core principles and practices adopted by professional social engineers to manipulate humans into divulging information or performing an act. You will learn some of the basic psychological principles that formulate the goals and vision of a social engineer. You will also learn about the attack process and methods of social engineering followed by real-world examples. In the end, you will be given hands-on exercise using the social engineering tools that can assist you in evaluating the target's human infrastructure.

Chapter 9, *Target Exploitation*, highlights the practices and tools that can be used to conduct a real-world exploitation. The chapter will explain what areas of vulnerability research are crucial in order to understand, examine, and test the vulnerability. Additionally, it will also point out several exploit repositories that should keep you informed about the publicly available exploits and when to use them. You will also learn to use one of the infamous exploitation toolkits from a target evaluation perspective. Moreover, you will discover the steps for writing a simple exploit module for the Metasploit framework.

Chapter 10, *Privilege Escalation*, introduces you to privilege escalation as well as network sniffing and spoofing. You will learn how to escalate your gained privilege using a local exploit. You will also learn the tools required to attack a password via the offline or online technique. You will also learn about several tools that can be used to spoof the network traffic. In the last part of this chapter, you will discover several tools that can be used to do a network sniffing attack.

Chapter 11, *Maintaining Access*, introduces you to the operating system and web backdoors. You will learn about several backdoors that are available and how to use them. You will also learn about several network tunneling tools that can be used to create covert communication between the attacker and the victim machine.