Kali Linux: Windows Penetration Testing

Kali Linux: a complete pen testing toolkit facilitating smooth backtracking for working hackers

Wolf Halton
Bo Weaver

DOWNLOAD EBOOK
Synopsis
Kali Linux: a complete pentesting toolkit facilitating smooth backtracking for working hackers

About This Book
Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux. Footprint, monitor, and audit your network and investigate any ongoing infestations. Customize Kali Linux with this professional guide so it becomes your pen testing toolkit.

Who This Book Is For
If you are a working ethical hacker who is looking to expand the offensive skillset with a thorough understanding of Kali Linux, then this is the book for you. Prior knowledge about Linux operating systems and the BASH terminal emulator along with Windows desktop and command line would be highly beneficial.

What You Will Learn
- Set up Kali Linux for pen testing
- Map and enumerate your Windows network
- Exploit several common Windows network vulnerabilities
- Attack and defeat password schemes on Windows
- Debug and reverse-engineer Windows programs
- Recover lost files, investigate successful hacks and discover hidden data in innocent-looking files
- Catch and hold admin rights on the network, and maintain backdoors on the network after your initial testing is done

In Detail
Microsoft Windows is one of the two most common OS and managing its security has spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Kali is built on the Debian distribution of Linux and shares the legendary stability of that OS. This lets you focus on using the network penetration, password cracking, forensics tools and not the OS.

This book has the most advanced tools and techniques to reproduce the methods used by sophisticated hackers to make you an expert in Kali Linux penetration testing. First, you are introduced to Kali’s top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities to be able to exploit a system remotely. Next, you will prove that the vulnerabilities you have found are real and exploitable. You will learn to use tools in seven categories of exploitation tools. Further, you perform web access exploits using tools like websploit and more.

Security is only as strong as the weakest link in the chain. Passwords are often that weak link. Thus, you learn about password attacks that can be used in concert with other approaches to break into and own a network. Moreover, you come to terms with network sniffing, which helps you understand which users are using services you can exploit, and IP spoofing, which can be used to poison a system’s DNS cache. Once you gain access to a machine or network, maintaining access is important. Thus, you not only learn penetrating in the machine you also learn Windows privilege’s escalations.

With easy to follow step-by-step instructions and support images, you will be able to quickly pen test your system and network.

Style and approach
This book is a hands-on guide for Kali Linux pen testing. This book will provide all the practical knowledge needed to test your network’s
security using a proven hacker's methodology. The book uses easy-to-understand yet professional language for explaining concepts.

**Book Information**

Paperback: 422 pages  
Publisher: Packt Publishing - ebooks Account (June 28, 2016)  
Language: English  
ISBN-10: 1782168494  
Product Dimensions: 7.5 x 1 x 9.2 inches  
Shipping Weight: 1.9 pounds (View shipping rates and policies)  
Average Customer Review: Be the first to review this item  

*Download to continue reading...*

Dmca