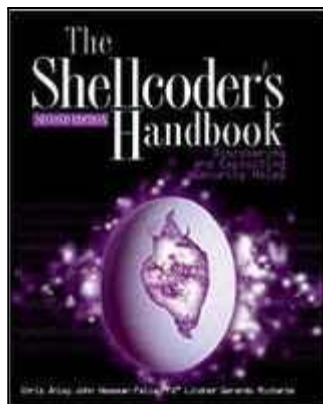
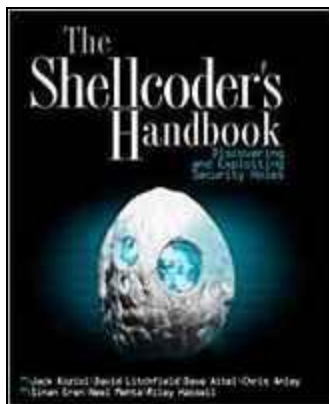


《Shellcoder 手册——发现和利用安全漏洞》



分类	IT 类 / 信息安全 / 入侵与渗透测试
作者 (第2版)	Chris Anley John Heasman Felix Lindner Gerardo Richarte
作者 (第1版)	Jack Koziol David Litchfield Dave Aitel
英文书名	《The Shellcoder's Handbook ——Discovering and Exploiting Security Holes》
出版年份	2004(第1版, 原著) 2007(第2版, 原著)

简介

此书第1版出版于2004年，第2版出版于2007年。两个版本的作者不一样(参见表格)。由于作者比较多，俺偷懒一下，就不逐一介绍了。

书中不仅讲了“如何编写 Shellcode”，还讲了“如何发现漏洞”和“如何利用漏洞”。涉及的操作系统平台包括了：Linux、Windows、Solaris、Mac OS、思科路由器。

英文目录(第2版)

About the Authors

Acknowledgments

Introduction to the Second Edition

Part I Introduction to Exploitation Linux on x86

- Chapter 1 Before You Begin
- Chapter 2 Stack Overflows
- Chapter 3 Shellcode
- Chapter 4 Introduction to Format String Bugs
- Chapter 5 Introduction to Heap Overflows

Part II Other Platforms—Windows, Solaris, OS/X, and Cisco

- Chapter 6 The Wild World of Windows
- Chapter 7 Windows Shellcode
- Chapter 8 Windows Overflows
- Chapter 9 Overcoming Filters
- Chapter 10 Introduction to Solaris Exploitation
- Chapter 11 Advanced Solaris Exploitation
- Chapter 12 OS X Shellcode
- Chapter 13 Cisco IOS Exploitation
- Chapter 14 Protection Mechanisms

Part III Vulnerability Discovery

- Chapter 15 Establishing a Working Environment
- Chapter 16 Fault Injection
- Chapter 17 The Art of Fuzzing
- Chapter 18 Source Code Auditing Finding Vulnerabilities in C-Based Languages
- Chapter 19 Instrumented Investigation A Manual Approach
- Chapter 20 Tracing for Vulnerabilities
- Chapter 21 Binary Auditing Hacking Closed Source Software

Part IV Advanced Materials

- Chapter 22 Alternative Payload Strategies
- Chapter 23 Writing Exploits that Work in the Wild
- Chapter 24 Attacking Database Software
- Chapter 25 Unix Kernel Overflows
- Chapter 26 Exploiting Unix Kernel Vulnerabilities
- Chapter 27 Hacking the Windows Kernel

Index

[【编程随想】收藏的电子书清单](#)

[【编程随想】的博客](#)