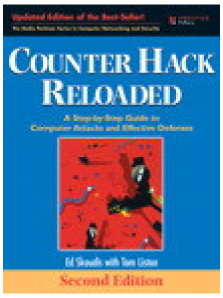
Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, 2/E



Edward Skoudis, with
Tom Liston

Publisher: Prentice Hall
Copyright: 2006
Format: Paper; 784 pp

ISBN-10: 0131481045
ISBN-13: 9780131481046

Our Price: £35.99
Status: Instock
Published: 05 Jan 2006

Description

For years, *Counter Hack* has been the primary resource for every network/system administrator and security professional who needs a deep, hands-on understanding of hacker attacks and countermeasures. Now, leading network security experts Ed Skoudis and Tom Liston have thoroughly updated this best-selling guide, showing how to defeat today's newest, most sophisticated, and most destructive attacks.

Table Of Contents

(NOTE: *Each chapter concludes with Summary*).

Foreword.
Preface Reloaded.
About the Authors.
1. Introduction.
The Computer World and the Golden Age of Hacking.
Why This Book?
The Threat: Never Underestimate Your Adversary.
A Note on Terminology and Iconography.
Caveat: These Tools Could Hurt You.
Organization of Rest of the Book.
2. Networking Overview: Pretty Much Everything You Need to Know About Networking to Follow the Rest of This Book.
The OSI Reference Model and Protocol Layering.
How Does TCP/IP Fit In?
Understanding TCP/IP.
Transmission Control Protocol (TCP).
User Datagram Protocol (UDP).
Internet Protocol (IP) and Internet Control Message Protocol (ICMP).
ICMP.
Other Network-Level Issues.
Don’t Forget About the Data Link and Physical Layers!
Security Solutions for the Internet.
Conclusion.
3. Linux and UNIX Overview: Pretty Much Everything You Need to Know About Linux and UNIX to Follow the Rest of This Book.
Introduction.
Architecture.
Accounts and Groups.
Linux and UNIX Permissions.
Linux and UNIX Trust Relationships.
Common Linux and UNIX Network Services.
Conclusion.
4. Windows NT/000/XP/00 Overview: Pretty Much Everything You Need to Know About Windows to Follow the Rest of This Book.
Introduction.
A Brief History of Time.
The Underlying Windows Operating System Architecture.

How Windows Password Representations Are Derived.
Kernel Mode.
From Service Packs and Hotfixes to Windows Update and Beyond.
Accounts and Groups.
Privilege Control.
Policies
Trust.
Auditing.
Object Access Control and Permissions.
Network Security.
Windows 2000 and Beyond: Welcome to the New Millennium.
Conclusion.
5. Phase 1: Reconnaissance.
Low-Technology Reconnaissance: Social Engineering, Caller ID Spoofing, Physical Break-In, and Dumpster Diving.
Search the Fine Web (STFW).
Who is Databases: Treasure Chests of Information.
The Domain Name System.
General-Purpose Reconnaissance Tools.
Conclusion.
6. Phase 2: Scanning.
War Driving: Finding Wireless Access Points.
War Dialing: Looking for Modems in All the Right Places.
Network Mapping.
Determining Open Ports Using Port Scanners.
Vulnerability-Scanning Tools.
Intrusion Detection System and Intrusion Prevention System Evasion.
Conclusion.
7. Phase 3: Gaining Access Using Application and Operating System Attacks.
Script Kiddie Exploit Trolling.
Pragmatism for More Sophisticated Attackers.
Buffer Overflow Exploits.
Password Attacks.
Web Application Attacks.
Exploiting Browser Flaws.
Conclusion.
8. Phase 4: Gaining Access Using Network Attacks.
Sniffing.
IP Address Spoofing.
Session Hijacking.
Netcat: A General-Purpose Network Tool.
Conclusion.
9. Phase 3: Denial-of-Service Attacks.
Locally Stopping Services.
Locally Exhausting Resources.
Remotely Stopping Services.
Remotely Exhausting Resources.
Conclusion.
10. Phase 4: Maintaining Access: Trojans, Backdoors, and Rootkits ... Oh My!
Trojan Horses.
Backdoors.
The Devious Duo: Backdoors Melded into Trojan Horses.
Nasty: Application-Level Trojan Horse Backdoor Tools.
Also Nasty: The Rise of the Bots.
Additional Nastiness: Spyware Everywhere!
Defenses Against Application-Level Trojan Horse Backdoors, Bots, and Spyware.
Even Nastier: User-Mode Rootkits.
Defending Against User-Mode Rootkits.
Nastiest: Kernel-Mode Rootkits.
Defending Against Kernel-Mode Rootkits.
Conclusion.
11. Phase 5: Covering Tracks and Hiding.
Hiding Evidence by Altering Event Logs.
Defenses Against Log and Accounting File Attacks.
Creating Difficult-to-Find Files and Directories.
Hiding Evidence on the Network: Covert Channels.
Defenses Against Covert Channels.
Conclusion.
12. Putting It All Together: Anatomy of an Attack.
Scenario 1: Crouching Wi-Fi, Hidden Dragon.
Scenario 2: Death of a Telecommuter.

Scenario 3: The Manchurian Contractor.
Conclusion.
13. The Future, References, and Conclusions.
Where Are We Heading?
Keeping Up to Speed.
Final Thoughts ... Live Long and Prosper.
Index.

Features

Major revision to the best-selling, step-by-step guide to defending against hacker intrusions--more than 45% new material.
° Contains more than 45% new material including coverage devoted to the steps of scanning, gaining and maintaining access, and preventing detection
° All new scenarios in the anatomy of an attack chapter and tools to battle them
° Author is a huge name in security. The first edition is touted as "outstanding" and the "best of its kind"

New To This Edition

Important features of this new edition include

- All-new "anatomy-of-an-attack" scenarios and tools
- All-new section on wireless hacking: wardriving, warchalking, WEP attacks, and more
- Fully updated coverage of reconnaissance tools, including Nmap port scanning and "Google hacking"
- New coverage of tools for gaining access, including uncovering Windows vulnerabilities with Mediasploit
- New information on dangerous, hard-to-detect, kernel-level rootkits

Appropriate Courses

CS1404 Network Security (PH) [PH PTR]

Instructor Supplements

PowerPoint Slides
Skoudis
© 2007 | Prentice Hall | Slides | Instock - Instructor only resource
ISBN-10: 013233352X | ISBN-13: 9780132333528