

Know Your Network

2nd Edition



Network Security Assessment

O'REILLY®

Chris McNab

Network Security Assessment

Other resources from O'Reilly

| | | |
|-----------------------|------------------------------------------------|----------------------------------|
| Related titles | Network Security Hacks | Security Power Tools |
| | Apache Security | Network Security with OpenSSL |
| | SSH, the Secure Shell: The Definitive Guide | Computer Security Basics |
| | | |

oreilly.com *oreilly.com* is more than a complete catalog of O'Reilly books. You'll also find links to news, events, articles, weblogs, sample chapters, and code examples.



oreillynet.com is the essential portal for developers interested in open and emerging technologies, including new platforms, programming languages, and operating systems.

Conferences O'Reilly brings diverse innovators together to nurture the ideas that spark revolutionary industries. We specialize in documenting the latest tools and systems, translating the innovator's knowledge into useful skills for those in the trenches. Visit *conferences.oreilly.com* for our upcoming events.



Safari Bookshelf (*safari.oreilly.com*) is the premier online reference library for programmers and IT professionals. Conduct searches across more than 1,000 books. Subscribers can zero in on answers to time-critical questions in a matter of seconds. Read the books on your Bookshelf from cover to cover or simply flip to the page you need. Try it today for free.

SECOND EDITION

Network Security Assessment

Chris McNab

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

Network Security Assessment, Second Edition

by Chris McNab

Copyright © 2008 Chris McNab. All rights reserved.
Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*safari.oreilly.com*). For more information, contact our corporate/institutional sales department: (800) 998-9938 or *corporate@oreilly.com*.

Editor: Tatiana Apanidi

Production Editor: Sarah Schneider

Copyeditor: Amy Thomson

Proofreader: Sarah Schneider

Indexer: Lucie Haskins

Cover Designer: Karen Montgomery

Interior Designer: David Futato

Illustrator: Robert Romano

Printing History:

March 2004: First Edition.

October 2007: Second Edition.

Nutshell Handbook, the Nutshell Handbook logo, and the O'Reilly logo are registered trademarks of O'Reilly Media, Inc. *Network Security Assessment*, the cover image, and related trade dress are trademarks of O'Reilly Media, Inc.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O'Reilly Media, Inc. was aware of a trademark claim, the designations have been printed in caps or initial caps.

While every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.



This book uses RepKover™, a durable and flexible lay-flat binding.

ISBN-10: 0-596-51030-6

ISBN-13: 978-0-596-51030-5

[M]

Table of Contents

| | |
|-------------------------------------------------------|-----------|
| Foreword | xi |
| Preface | xv |
| 1. Network Security Assessment | 1 |
| The Business Benefits | 1 |
| IP: The Foundation of the Internet | 2 |
| Classifying Internet-Based Attackers | 2 |
| Assessment Service Definitions | 3 |
| Network Security Assessment Methodology | 4 |
| The Cyclic Assessment Approach | 8 |
| 2. Network Security Assessment Platform | 10 |
| Virtualization Software | 10 |
| Operating Systems | 11 |
| Reconnaissance Tools | 13 |
| Network Scanning Tools | 13 |
| Exploitation Frameworks | 14 |
| Web Application Testing Tools | 16 |
| 3. Internet Host and Network Enumeration | 17 |
| Querying Web and Newsgroup Search Engines | 18 |
| Querying Domain WHOIS Registrars | 20 |
| Querying IP WHOIS Registrars | 23 |
| BGP Querying | 28 |
| DNS Querying | 30 |
| Web Server Crawling | 37 |
| Automating Enumeration | 37 |

| | |
|-------------------------------------------------------|------------|
| SMTP Probing | 38 |
| Enumeration Technique Recap | 39 |
| Enumeration Countermeasures | 40 |
| 4. IP Network Scanning | 42 |
| ICMP Probing | 42 |
| TCP Port Scanning | 49 |
| UDP Port Scanning | 60 |
| IDS Evasion and Filter Circumvention | 62 |
| Low-Level IP Assessment | 71 |
| Network Scanning Recap | 76 |
| Network Scanning Countermeasures | 77 |
| 5. Assessing Remote Information Services | 79 |
| Remote Information Services | 79 |
| DNS | 80 |
| Finger | 86 |
| Auth | 88 |
| NTP | 89 |
| SNMP | 91 |
| LDAP | 95 |
| rwho | 98 |
| RPC rusers | 98 |
| Remote Information Services Countermeasures | 99 |
| 6. Assessing Web Servers | 101 |
| Web Servers | 101 |
| Fingerprinting Accessible Web Servers | 102 |
| Identifying and Assessing Reverse Proxy Mechanisms | 107 |
| Enumerating Virtual Hosts and Web Sites | 113 |
| Identifying Subsystems and Enabled Components | 114 |
| Investigating Known Vulnerabilities | 132 |
| Basic Web Server Crawling | 155 |
| Web Servers Countermeasures | 158 |
| 7. Assessing Web Applications | 160 |
| Web Application Technologies Overview | 160 |
| Web Application Profiling | 161 |
| Web Application Attack Strategies | 170 |

| | |
|--------------------------------------------------------|------------|
| Web Application Vulnerabilities | 180 |
| Web Security Checklist | 196 |
| 8. Assessing Remote Maintenance Services | 198 |
| Remote Maintenance Services | 198 |
| FTP | 199 |
| SSH | 212 |
| Telnet | 215 |
| R-Services | 220 |
| X Windows | 224 |
| Citrix | 229 |
| Microsoft Remote Desktop Protocol | 232 |
| VNC | 234 |
| Remote Maintenance Services Countermeasures | 237 |
| 9. Assessing Database Services | 239 |
| Microsoft SQL Server | 239 |
| Oracle | 244 |
| MySQL | 252 |
| Database Services Countermeasures | 255 |
| 10. Assessing Windows Networking Services | 256 |
| Microsoft Windows Networking Services | 256 |
| Microsoft RPC Services | 257 |
| The NetBIOS Name Service | 273 |
| The NetBIOS Datagram Service | 275 |
| The NetBIOS Session Service | 276 |
| The CIFS Service | 285 |
| Unix Samba Vulnerabilities | 287 |
| Windows Networking Services Countermeasures | 288 |
| 11. Assessing Email Services | 290 |
| Email Service Protocols | 290 |
| SMTP | 290 |
| POP-2 and POP-3 | 302 |
| IMAP | 303 |
| Email Services Countermeasures | 305 |

| | |
|----------------------------------------------|------------|
| 12. Assessing IP VPN Services | 307 |
| IPsec VPNs | 307 |
| Attacking IPsec VPNs | 311 |
| Microsoft PPTP | 320 |
| SSL VPNs | 321 |
| VPN Services Countermeasures | 329 |
| 13. Assessing Unix RPC Services | 330 |
| Enumerating Unix RPC Services | 330 |
| RPC Service Vulnerabilities | 332 |
| Unix RPC Services Countermeasures | 339 |
| 14. Application-Level Risks | 340 |
| The Fundamental Hacking Concept | 340 |
| Why Software Is Vulnerable | 341 |
| Network Service Vulnerabilities and Attacks | 342 |
| Classic Buffer-Overflow Vulnerabilities | 346 |
| Heap Overflows | 356 |
| Integer Overflows | 364 |
| Format String Bugs | 367 |
| Memory Manipulation Attacks Recap | 373 |
| Mitigating Process Manipulation Risks | 374 |
| Recommended Secure Development Reading | 376 |
| 15. Running Nessus | 377 |
| Nessus Architecture | 377 |
| Deployment Options and Prerequisites | 378 |
| Nessus Installation | 379 |
| Configuring Nessus | 383 |
| Running Nessus | 389 |
| Nessus Reporting | 390 |
| Running Nessus Recap | 392 |
| 16. Exploitation Frameworks | 393 |
| Metasploit Framework | 393 |
| CORE IMPACT | 400 |
| Immunity CANVAS | 408 |
| Exploitation Frameworks Recap | 414 |

| | |
|--------------------------------------------------------|------------|
| A. TCP, UDP Ports, and ICMP Message Types | 415 |
| B. Sources of Vulnerability Information | 420 |
| C. Exploit Framework Modules | 422 |
| Index | 453 |