

Contents at a Glance

Foreword	xvii
Introduction	1
Part I: Building the Foundation for Ethical Hacking	7
Chapter 1: Introduction to Ethical Hacking	9
Chapter 2: Cracking the Hacker Mindset.....	23
Chapter 3: Developing Your Ethical Hacking Plan.....	33
Chapter 4: Hacking Methodology	45
Part II: Putting Ethical Hacking in Motion	59
Chapter 5: Social Engineering	61
Chapter 6: Physical Security	75
Chapter 7: Passwords	85
Part III: Hacking the Network	113
Chapter 8: War Dialing	115
Chapter 9: Network Infrastructure	127
Chapter 10: Wireless LANs	161
Part IV: Hacking Operating Systems	187
Chapter 11: Windows	189
Chapter 12: Linux	221
Chapter 13: Novell NetWare	243
Part V: Hacking Applications	263
Chapter 14: Messaging Systems	265
Chapter 15: Web Applications	293
Part VI: Ethical Hacking Aftermath	325
Chapter 16: Reporting Your Results.....	327
Chapter 17: Plugging Security Holes	333
Chapter 18: Managing Security Changes	339
Part VII: The Part of Tens	345
Chapter 19: Ten Tips for Getting Upper Management Buy-In.....	347
Chapter 20: Ten Deadly Mistakes	353
Appendix: Tools and Resources	357
Index	371

Table of Contents

Forewordxvii

Introduction 1

Who Should Read This Book?.....1
About This Book.....2
How to Use This Book2
What You Don't Need to Read3
Foolish Assumptions3
How This Book Is Organized.....3
 Part I: Building the Foundation for Ethical Hacking.....4
 Part II: Putting Ethical Hacking in Motion4
 Part III: Hacking the Network.....4
 Part IV: Hacking Operating Systems4
 Part V: Hacking Applications5
 Part VI: Ethical Hacking Aftermath5
 Part VII: The Part of Tens5
Icons Used in This Book.....6
Where to Go from Here.....6

Part I: Building the Foundation for Ethical Hacking..... 7

Chapter 1: Introduction to Ethical Hacking 9

Straightening Out the Terminology9
 Defining hacker10
 Defining rogue insider.....11
How Malicious Attackers Beget Ethical Hackers11
Understanding the Need to Hack Your Own Systems12
Understanding the Dangers Your Systems Face13
 Nontechnical attacks14
 Network infrastructure attacks14
 Operating system attacks.....14
 Application and other specialized attacks.....15
Obeying the Ethical Hacking Commandments15
 Working ethically.....16
 Respecting privacy.....16
 Not crashing your systems16
The Ethical Hacking Process17
 Formulating your plan17
 Selecting tools.....19



Executing the plan.....	21
Evaluating results.....	22
Moving on.....	22
Chapter 2: Cracking the Hacker Mindset	23
What You're Up Against.....	23
Who Breaks into Computer Systems	26
Why They Do It.....	28
Planning and Performing Attacks.....	30
Maintaining Anonymity	32
Chapter 3: Developing Your Ethical Hacking Plan	33
Getting Your Plan Approved.....	33
Establishing Your Goals.....	34
Determining Which Systems to Hack	36
Creating Testing Standards.....	39
Timing	39
Specific tests	40
Blind versus knowledge assessments	41
Location.....	41
Reacting to major vulnerabilities that you find.....	42
Silly assumptions.....	42
Selecting Tools.....	43
Chapter 4: Hacking Methodology	45
Setting the Stage.....	45
Seeing What Others See	47
Gathering public information	47
Mapping the network.....	49
Scanning Systems.....	52
Hosts	52
Modems and open ports	53
Determining What's Running on Open Ports.....	53
Assessing Vulnerabilities	55
Penetrating the System	57
<i>Part II: Putting Ethical Hacking in Motion</i>	<i>59</i>
Chapter 5: Social Engineering	61
Social Engineering 101.....	61
Before You Start.....	62
Why Attackers Use Social Engineering.....	64
Understanding the Implications.....	65
Performing Social Engineering Attacks	66
Fishing for information	66
Building trust	68
Exploiting the relationship.....	69

Social Engineering Countermeasures	72
Policies.....	72
User awareness and training.....	72
Chapter 6: Physical Security	75
Physical Security Vulnerabilities	75
What to Look For.....	76
Building infrastructure	78
Utilities.....	79
Office layout and usage	80
Network components and computers	81
Chapter 7: Passwords	85
Password Vulnerabilities.....	86
Organizational password vulnerabilities.....	86
Technical password vulnerabilities	88
Cracking Passwords.....	88
Cracking passwords the old-fashioned way	89
High-tech password cracking.....	91
Password-protected files.....	102
Other ways to crack passwords	103
General Password-Cracking Countermeasures	108
Storing passwords.....	108
Policy considerations	109
Other considerations	110
Securing Operating Systems.....	111
Windows	111
Linux and UNIX.....	112
 Part III: Hacking the Network.....	 113
Chapter 8: War Dialing	115
Modem Safety	115
General Telephone System Vulnerabilities	116
Attacking Systems by War Dialing.....	116
Gathering information	118
Selecting war dialing tools	119
Dialing in from the outside.....	120
Using tools.....	121
Rooting through the systems.....	124
War Dialing Countermeasures	125
Phone numbers.....	125
Modem operation.....	125
Installation.....	126

Chapter 9: Network Infrastructure127

Network Infrastructure Vulnerabilities	129
Choosing Tools	130
Scanners and analyzers	130
Vulnerability assessment	131
Scanning, Poking, and Prodding.....	131
Port scanners.....	132
SNMP scanning.....	139
Banner grabbing.....	142
Firewall rules.....	143
Network analyzers.....	146
The MAC-daddy attack	153
Denial of service.....	157
General Network Defenses.....	159

Chapter 10: Wireless LANs161

Understanding the Implications of Wireless Network Vulnerabilities.....	161
Choosing Your Tools.....	162
Wireless LAN Discovery	165
Checking for worldwide recognition.....	165
Scanning your local airwaves	167
Wireless Network Attacks	168
Encrypted traffic	168
Countermeasures against encrypted traffic attacks.....	172
Rogue wireless devices.....	173
Countermeasures against rogue wireless devices	178
MAC spoofing.....	179
Countermeasures against MAC spoofing	183
Queensland DoS attack.....	183
Countermeasures against DoS attacks	184
Physical security problems.....	184
Countermeasures against physical security problems	184
Vulnerable wireless workstations	185
Countermeasures against vulnerable wireless workstations	185
Default configuration settings	186
Countermeasures against default configuration settings exploits.....	186

Part IV: Hacking Operating Systems..... 187**Chapter 11: Windows189**

Windows Vulnerabilities	190
Choosing Tools	190
Essential tools.....	191
Free Microsoft tools	191

All-in-one assessment tools.....192
 Task-specific tools192
 Information Gathering193
 System scanning.....194
 NetBIOS.....196
 RPC.....199
 Enumeration.....200
 Countermeasures against RPC enumeration200
 Null Sessions.....201
 Hacks.....201
 Countermeasures against null session hacks206
 Share Permissions.....208
 Windows defaults208
 Testing209
 Hardcore Vulnerability Exploitation210
 Using Metasploit.....212
 Using CORE IMPACT.....215
 Countermeasures against hardcore vulnerability exploits.....217
 Authenticated Scans218
 General OS vulnerabilities.....218
 Rooting out sensitive text in network files.....219

Chapter 12: Linux221

Linux Vulnerabilities.....222
 Choosing Tools222
 Information Gathering223
 System scanning.....223
 Countermeasures against system scanning.....227
 Unneeded Services227
 Searches.....227
 Countermeasures against attacks on unneeded services.....229
 .rhosts and hosts.equiv Files231
 Hacks using the .rhosts and hosts.equiv files231
 Countermeasures against .rhosts and hosts.equiv file attacks...232
 NFS233
 NFS hacks234
 Countermeasures against NFS attacks235
 File Permissions235
 File permission hacks236
 Countermeasures against file permission attacks236
 Buffer Overflows237
 Attacks237
 Countermeasures against buffer-overflow attacks238
 Physical Security.....238
 Physical security hacks238
 Countermeasures against physical security attacks238
 General Security Tests.....239
 Patching Linux.....241

Distribution updates	241
Multiplatform update managers	242
Chapter 13: Novell NetWare	243
NetWare Vulnerabilities	243
Choosing Tools	244
Getting Started	244
Server access methods	245
Port scanning	245
NCPQuery	247
Countermeasures against enumeration	248
Authentication	248
rconsole	249
Server-console access	251
Intruder detection	252
Rogue NLMs	253
Cleartext packets	257
Solid Practices for Minimizing NetWare Security Risks	258
Rename admin	258
Disable eDirectory browsing	259
Remove bindery contexts	260
Audit the system	261
TCP/IP parameters	261
Patch	262
 Part V: Hacking Applications	 263
 Chapter 14: Messaging Systems	 265
Messaging System Vulnerabilities	265
E-Mail Attacks	266
E-mail bombs	268
Banners	271
SMTP attacks	272
General best practices for minimizing e-mail security risks	280
Instant Messaging	281
IM vulnerabilities	281
Countermeasures against IM vulnerabilities	284
Voice over IP	286
VoIP vulnerabilities	286
Countermeasures against VoIP vulnerabilities	292
 Chapter 15: Web Applications and Databases	 293
Choosing Your Web Application Tools	294
Web Application Vulnerabilities	294
Unsecured login mechanisms	296
Countermeasures against unsecured login systems	298
Directory traversal	299

Countermeasures against directory traversals302
 Input filtering attacks303
 Countermeasures against input attacks309
 Memory attacks310
 Countermeasures against memory attacks311
 Default script attacks312
 Countermeasures against default script attacks312
 URL filter bypassing313
 Countermeasures against URL filter bypassing315
 General security scans for Web application vulnerabilities315
 Database Vulnerabilities316
 Finding database servers on the network.....317
 Cracking database server passwords.....318
 Scanning databases for vulnerabilities.....320
 General Best Practices for Minimizing Security Risks.....322
 Obscurity.....322
 Firewalls.....323

Part VI: Ethical Hacking Aftermath325

Chapter 16: Reporting Your Results327

Pulling the Results Together.....327
 Prioritizing Vulnerabilities329
 Reporting Methods330

Chapter 17: Plugging Security Holes333

Turning Your Reports into Action.....333
 Patching for Perfection.....334
 Patch management.....334
 Patch automation335
 Hardening Your Systems336
 Assessing Your Security Infrastructure.....337

Chapter 18: Managing Security Changes339

Automating the Ethical Hacking Process339
 Monitoring Malicious Use340
 Outsourcing Ethical Hacking341
 Instilling a Security-Aware Mindset343
 Keeping Up with Other Security Issues.....344

Part VII: The Part of Tens.....345

Chapter 19: Ten Tips for Getting Upper Management Buy-In347

Chapter 20: Ten Deadly Mistakes353

<i>Appendix: Tools and Resources</i>	357
Awareness and Training	357
Bluetooth.....	358
Certifications	358
Dictionary Files and Word Lists	358
Exploit Tools	358
General Research Tools.....	359
Hacker Stuff.....	360
Linux	360
Log Analysis.....	361
Malware	361
Messaging.....	361
NetWare	362
Networks	362
Password Cracking.....	364
Patch Management	364
Source Code Analysis	365
Security Standards	365
Security Education.....	366
Storage.....	366
Risk Analysis and Threat Modeling	366
Voice over IP	366
War Dialing.....	367
Web Applications and Databases.....	367
Windows	368
Wireless Networks	369
<i>Index</i>	371