

Table of Contents

Foreword	xvii
-----------------------	-------------

Introduction	1
---------------------------	----------

Who Should Read This Book?	1
About This Book	2
How to Use This Book	2
What You Don't Need to Read	3
Foolish Assumptions	3
How This Book Is Organized	3
Part I: Building the Foundation for Ethical Hacking	4
Part II: Putting Ethical Hacking in Motion	4
Part III: Network Hacking	4
Part IV: Operating System Hacking	4
Part V: Application Hacking	5
Part VI: Ethical Hacking Aftermath	5
Part VII: The Part of Tens	5
Part VIII: Appendixes	5
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
---	----------

How Hackers Beget Ethical Hackers	9
Defining hacker	9
Ethical Hacking 101	10
Understanding the Need to Hack Your Own Systems	11
Understanding the Dangers Your Systems Face	12
Nontechnical attacks	12
Network-infrastructure attacks	13
Operating-system attacks	13
Application and other specialized attacks	13
Obeying the Ethical hacking Commandments	14
Working ethically	14
Respecting privacy	14
Not crashing your systems	15
The Ethical hacking Process	15
Formulating your plan	15
Selecting tools	17
Executing the plan	19
Evaluating results	20
Moving on	20



Chapter 2: Cracking the Hacker Mindset	21
What You're Up Against	21
Who Hacks	22
Why Hackers Hack	24
Planning and Performing Attacks	26
Maintaining Anonymity	27
Chapter 3: Developing Your Ethical Hacking Plan	29
Getting Your Plan Approved	29
Establishing Your Goals	30
Determining What Systems to Hack	32
Creating Testing Standards	33
Timing	34
Specific tests	34
Blind versus knowledge assessments	35
Location	36
Reacting to major exploits that you find	36
Silly assumptions	36
Selecting Tools	37
Chapter 4: Hacking Methodology	39
Setting the Stage	39
Seeing What Others See	41
Gathering public information	41
Mapping the network	43
Scanning Systems	45
Hosts	46
Modems and open ports	46
Determining What's Running on Open Ports	47
Assessing Vulnerabilities	49
Penetrating the System	51

Part II: Putting Ethical Hacking in Motion53

Chapter 5: Social Engineering	55
Social Engineering 101	55
Before You Start	56
Why Hackers Use Social Engineering	58
Understanding the Implications	58
Performing Social-Engineering Attacks	59
Fishing for information	60
Building trust	62
Exploiting the relationship	63
Social-Engineering Countermeasures	65
Policies	66
User awareness	66

Chapter 6: Physical Security	69
Physical-Security Vulnerabilities	69
What to Look For	70
Building infrastructure	72
Utilities	73
Office layout and usage	74
Network components and computers	75
Chapter 7: Passwords	79
Password Vulnerabilities	79
Organizational password vulnerabilities	80
Technical password vulnerabilities	82
Cracking Passwords	82
Cracking passwords the old-fashioned way	83
High-tech password cracking	85
General password-hacking countermeasures	91
Password-protected files	95
Other ways to crack passwords	97
Securing Operating Systems	101
Windows	101
Linux and UNIX	102
 Part III: Network Hacking	 103
Chapter 8: War Dialing	105
War Dialing	105
Modem safety	105
General telephone-system vulnerabilities	106
Attacking	106
Countermeasures	114
Chapter 9: Network Infrastructure	117
Network Infrastructure Vulnerabilities	119
Choosing Tools	120
Scanners	120
Vulnerability assessment	121
Scanning, Poking, and Prodding	121
Port scanners	121
SNMP scanning	129
Banner grabbing	130
Firewall rules	131
Looking through a network analyzer	134
The MAC-daddy attack	140
Denial of service	144
General network defenses	146

Chapter 10: Wireless LANs147

Understanding the Implications of Wireless Network Vulnerabilities	147
Choosing Your Tools	148
Wireless LAN Discovery	151
Checking for worldwide recognition	151
Scanning your local airwaves	152
Wireless Network Attacks	154
Encrypted traffic	155
Countermeasures	156
Rogue networks	158
Countermeasures	159
Physical-security problems	160
Countermeasures	160
Vulnerable wireless workstations	161
Countermeasures	161
Default configuration settings	162
Countermeasures	163

Part IV: Operating System Hacking 165**Chapter 11: Windows167**

Windows Vulnerabilities	168
Choosing Tools	168
Essential tools	169
Free Microsoft tools	169
All-in-one assessment tools	170
Task-specific tools	170
Information Gathering	171
System scanning	171
NetBIOS	174
RPC	177
Enumeration	178
Countermeasures	178
Null Sessions	179
HACKS	179
Countermeasures	184
Share Permissions	186
Windows defaults	186
Testing	187
General Security Tests	189
Windows Update	189
Microsoft Baseline Security Analyzer (MBSA)	190
LANguard	191

Chapter 12: Linux193

Linux Vulnerabilities	194
Choosing Tools	194

Information Gathering	195
System scanning	195
Countermeasures	199
Unneeded Services	200
Searches	200
Countermeasures	202
.rhosts and hosts.equiv Files	204
Hacks	204
Countermeasures	205
NFS	206
Hacks	206
Countermeasures	207
File Permission	207
Hacks	207
Countermeasures	207
Buffer Overflows	208
Attacks	209
Countermeasures	209
Physical Security	209
Hacks	210
Countermeasures	210
General Security Tests	211
Patching Linux	212
Distribution updates	213
Multiplatform update managers	213
Chapter 13: Novell NetWare	215
NetWare Vulnerabilities	215
Choosing Tools	216
Getting Started	216
Server access methods	217
Port scanning	217
NCPQuery	219
Countermeasures	220
Authentication	220
Rconsole	221
Server-console access	224
Intruder detection	224
Rogue NLMs	225
Clear-text packets	229
General Best Practices for Minimizing NetWare Security Risks	230
Rename admin	231
Disable eDirectory browsing	231
Removing bindery contexts	233
System auditing	233
TCP/IP parameters	234
Patching	234

Part V: Application Hacking235**Chapter 14: Malware237**

Implications of Malware Attacks	237
Types of Malware	239
Trojan horses	239
Viruses	240
Worms	240
Rootkits	240
Spyware	241
Built-in programming interfaces	241
Logic bombs	242
Security tools	242
How Malware Propagates	243
Automation	243
E-mail	243
Hacker backdoors	244
Testing	244
Vulnerable malware ports	244
Manual assessment	245
Antivirus software testing	249
Network scanning	250
Behavioral-analysis tools	253
Malware Countermeasures	253
General system administration	253
E-mails	255
Files	255

Chapter 15: Messaging Systems257

Messaging-System Vulnerabilities	257
E-Mail Attacks	258
E-mail bombs	258
Banners	263
SMTP attacks	265
General best practices for minimizing e-mail security risks	271
Instant Messaging	272
Vulnerabilities	272
Countermeasures	275

Chapter 16: Web Applications279

Web-Application Vulnerabilities	279
Choosing Your Tools	280
Insecure Login Mechanisms	280
Testing	280
Countermeasures	283
Directory Traversal	283
Testing	283
Countermeasures	285

Input Filtering	285
Input attacks	286
Countermeasures	289
Default Scripts	289
Attacks	289
Countermeasures	290
URL Filter Bypassing	290
Bypassing filters	290
Countermeasures	292
Automated Scans	292
Nikto	292
WebInspect	292
General Best Practices for Minimizing	
Web-Application Security Risks	294
Obscurity	294
Firewalls	295
 Part VI: Ethical Hacking Aftermath	297
Chapter 17: Reporting Your Results	299
Pulling the Results Together	299
Prioritizing Vulnerabilities	301
Reporting Methods	302
Chapter 18: Plugging Security Holes	305
Turning Your Reports into Action	305
Patching for Perfection	306
Patch management	306
Patch automation	307
Hardening Your Systems	308
Assessing Your Security Infrastructure	309
Chapter 19: Managing Security Changes	311
Automating the Ethical Hacking Process	311
Monitoring Malicious Use	312
Outsourcing Ethical Hacking	313
Instilling a Security-Aware Mindset	315
Keeping Up with Other Security Issues	316
 Part VII: The Part of Tens	317
Chapter 20: Ten Tips for Getting Upper Management Buy-In	319
Cultivate an Ally and Sponsor	319
Don't Be a FUDdy Duddy	319
Demonstrate How the Organization Can't Afford to Be Hacked	320
Outline the General Benefits of Ethical Hacking	320

Show How Ethical Hacking Specifically Helps the Organization	321
Get Involved in the Business	321
Establish Your Credibility	321
Speak on Their Level	322
Show Value in Your Efforts	322
Be Flexible and Adaptable	322
Chapter 21: Ten Deadly Mistakes	323
Not Getting Approval in Writing	323
Assuming That You Can Find All Vulnerabilities During Your Tests	324
Assuming That You Can Eliminate All Security Vulnerabilities	324
Performing Tests Only Once	324
Pretending to Know It All	325
Running Your Tests without Looking at Things from a Hacker's Viewpoint	325
Ignoring Common Attacks	325
Not Using the Right Tools	325
Pounding Production Systems at the Wrong Time	326
Outsourcing Testing and Not Staying Involved	326
 Part VIII: Appendixes	 327
Appendix A: Tools and Resources	329
Awareness and Training	329
Dictionary Files and Word Lists	329
General Research Tools	330
Hacker Stuff	330
Linux	331
Log Analysis	331
Malware	331
Messaging	332
NetWare	332
Networks	332
Password Cracking	333
War Dialing	334
Web Applications	334
Windows	334
Wireless Networks	335
 Appendix B: About the Book Web Site	 337
 Index	 339