

Contents at a Glance

<i>Foreword</i>	<i>xvii</i>
<i>Introduction</i>	<i>1</i>
<i>Part I: Building the Foundation for Testing Wireless Networks</i>	<i>7</i>
Chapter 1: Introduction to Wireless Hacking	9
Chapter 2: The Wireless Hacking Process	19
Chapter 3: Implementing a Testing Methodology	31
Chapter 4: Amassing Your War Chest	43
<i>Part II: Getting Rolling with Common Wi-Fi Hacks</i>	<i>65</i>
Chapter 5: Human (In)Security	67
Chapter 6: Containing the Airwaves	81
Chapter 7: Hacking Wireless Clients	97
Chapter 8: Discovering Default Settings	113
Chapter 9: Wardriving	131
<i>Part III: Advanced Wi-Fi Hacks</i>	<i>153</i>
Chapter 10: Still at War	155
Chapter 11: Unauthorized Wireless Devices	177
Chapter 12: Network Attacks	195
Chapter 13: Denial-of-Service Attacks	225
Chapter 14: Cracking Encryption	255
Chapter 15: Authenticating Users	281
<i>Part IV: The Part of Tens</i>	<i>301</i>
Chapter 16: Ten Essential Tools for Hacking Wireless Networks	303
Chapter 17: Ten Wireless Security-Testing Mistakes	307
Chapter 18: Ten Tips for Following Up after Your Testing	321
<i>Part V: Appendixes</i>	<i>325</i>
Appendix A: Wireless Hacking Resources	327
Appendix B: Glossary of Acronyms	341
<i>Index</i>	<i>347</i>

Table of Contents

Forewordxvii

Introduction 1

Who Should Read This Book?2
About This Book2
How to Use This Book2
Foolish Assumptions3
How This Book Is Organized3
 Part I: Building the Foundation for Testing Wireless Networks4
 Part II: Getting Rolling with Common Wi-Fi Hacks4
 Part III: Advanced Wi-Fi Hacks4
 Part IV: The Part of Tens5
 Part V: Appendixes5
Icons Used in This Book5
Where to Go from Here6

*Part I: Building the Foundation
for Testing Wireless Networks* 7

Chapter 1: Introduction to Wireless Hacking 9

Why You Need to Test Your Wireless Systems10
 Knowing the dangers your systems face11
 Understanding the enemy12
 Wireless-network complexities14
Getting Your Ducks in a Row15
Gathering the Right Tools16
To Protect, You Must Inspect17
 Non-technical attacks17
 Network attacks18
 Software attacks18

Chapter 2: The Wireless Hacking Process 19

Obeying the Ten Commandments of Ethical Hacking19
 Thou shalt set thy goals20
 Thou shalt plan thy work, lest thou go off course21
 Thou shalt obtain permission21
 Thou shalt work ethically22
 Thou shalt keep records22



- Thou shalt respect the privacy of others23
- Thou shalt do no harm23
- Thou shalt use a “scientific” process24
- Thou shalt not covet thy neighbor’s tools24
- Thou shalt report all thy findings25
- Understanding Standards26
 - Using ISO 1779926
 - Using CobiT27
 - Using SSE-CMM27
 - Using ISSAF27
 - Using OSSTMM28

Chapter 3: Implementing a Testing Methodology 31

- Determining What Others Know32
 - What you should look for32
 - Footprinting: Gathering what’s in the public eye33
- Mapping Your Network35
- Scanning Your Systems37
- Determining More about What’s Running39
- Performing a Vulnerability Assessment39
 - Manual assessment40
 - Automatic assessment40
 - Finding more information41
- Penetrating the System41

Chapter 4: Amassing Your War Chest 43

- Choosing Your Hardware44
 - The personal digital assistant44
 - The portable or laptop44
- Hacking Software45
 - Using software emulators45
 - Linux distributions on CD55
 - Stumbling tools56
 - You got the sniffers?56
- Picking Your Transceiver57
 - Determining your chipset57
 - Buying a wireless NIC59
- Extending Your Range59
- Using GPS62
- Signal Jamming63

Part II: Getting Rolling with Common Wi-Fi Hacks65

Chapter 5: Human (In)Security 67

- What Can Happen68
- Ignoring the Issues69

Social Engineering	70
Passive tests	71
Active tests	73
Unauthorized Equipment	74
Default Settings	76
Weak Passwords	77
Human (In)Security Countermeasures	78
Enforce a wireless security policy	78
Train and educate	79
Keep people in the know	79
Scan for unauthorized equipment	80
Secure your systems from the start	80
Chapter 6: Containing the Airwaves	81
Signal Strength	81
Using Linux Wireless Extension and Wireless Tools	81
Using Wavemon	87
Using Wscan	88
Using Wmap	88
Using XNetworkStrength	88
Using Wimon	88
Other link monitors	88
Network Physical Security Countermeasures	90
Checking for unauthorized users	90
Antenna type	91
Adjusting your signal strength	94
Chapter 7: Hacking Wireless Clients	97
What Can Happen	98
Probing for Pleasure	99
Port scanning	99
Using VPNMonitor	102
Looking for General Client Vulnerabilities	103
Common AP weaknesses	104
Linux application mapping	105
Windows null sessions	106
Ferretting Out WEP Keys	109
Wireless Client Countermeasures	111
Chapter 8: Discovering Default Settings	113
Collecting Information	113
Are you for Ethereal?	113
This is AirTraf control, you are cleared to sniff	114
Let me AiroPeek at your data	114
Another CommView of your data	115
Gulpit	117
That's Mognet not magnet	119
Other analyzers	119

Cracking Passwords	120
Using Cain & Abel	120
Using dsniff	124
Gathering IP Addresses	125
Gathering SSIDs	126
Using essid_jack	127
Using SSIDsniff	128
Default-Setting Countermeasures	128
Change SSIDs	128
Don't broadcast SSIDs	129
Using pong	129
Detecting sniffers	129

Chapter 9: Wardriving131

Introducing Wardriving	131
Installing and Running NetStumbler	133
Setting Up NetStumbler	134
Interpreting the Results	141
Mapping Your Stumbling	148
Using StumbVerter and MapPoint	149
Using Microsoft Streets & Trips	150
Using DiGLE	151

Part III: Advanced Wi-Fi Hacks 153**Chapter 10: Still at War155**

Using Advanced Wardriving Software	155
Installing and using Kismet	156
Installing and using Wellenreiter	167
Using WarLinux	168
Installing and using MiniStumbler	170
Using other wardriving software	173
Organization Wardriving Countermeasures	174
Using Kismet	174
Disabling probe responses	175
Increasing beacon broadcast intervals	175
Fake 'em out with a honeypot	175

Chapter 11: Unauthorized Wireless Devices177

What Can Happen	178
Wireless System Configurations	179
Characteristics of Unauthorized Systems	181
Wireless Client Software	184
Stumbling Software	186

Network-Analysis Software188
 Browsing the network188
 Probing further191
 Additional Software Options193
 Online Databases193
 Unauthorized System Countermeasures193

Chapter 12: Network Attacks195

What Can Happen196
 MAC-Address Spoofing197
 Changing your MAC in Linux198
 Tweaking your Windows settings199
 SMAC'ing your address203
 A walk down MAC-Spoofing Lane204
 Who's that Man in the Middle?208
 Management-frame attacks209
 ARP-poisoning attacks211
 SNMP: That's Why They Call It Simple213
 All Hail the Queensland Attack217
 Sniffing for Network Problems218
 Network-analysis programs218
 Network analyzer tips219
 Weird stuff to look for220
 Network Attack Countermeasures222

Chapter 13: Denial-of-Service Attacks225

What Can Happen227
 Types of DoS attacks227
 It's so easy228
 We Be Jamming229
 Common signal interrupters230
 What jamming looks like230
 Fight the power generators232
 AP Overloading234
 Guilty by association234
 Too much traffic240
 Are You Dis'ing Me?241
 Disassociations242
 Deauthentications242
 Invalid authentications via fata_jack249
 Physical Insecurities250
 DoS Countermeasures251
 Know what's normal251
 Contain your radio waves251
 Limit bandwidth253
 Use a Network Monitoring System253

Use a WIDS	253
Attack back	254
Demand fixes	254
Chapter 14: Cracking Encryption	255
What Can Happen	255
Protecting Message Privacy	256
Protecting Message Integrity	256
Using Encryption	257
WEP Weaknesses	259
Other WEP Problems to Look For	261
Attacking WEP	263
Active traffic injection	263
Active attack from both sides	263
Table-based attack	264
Passive attack decryption	264
Cracking Keys	264
Using WEPcrack	265
Using AirSnort	267
Using aircrack	269
Using WepLab	273
Finding other tools	274
Countermeasures Against Home Network-Encryption Attacks	274
Rotating keys	275
Using WPA	275
Organization Encryption Attack Countermeasures	277
Using WPA2	278
Using a VPN	278
Chapter 15: Authenticating Users	281
Three States of Authentication	281
Authentication according to IEEE 802.11	282
I Know Your Secret	283
Have We Got EAP?	284
This method seems easy to digest	285
Not another PEAP out of you	286
Another big LEAP for mankind	286
That was EAP-FAST	287
Beam me up, EAP-TLS	287
EAP-TTLS: That's funky software	288
Implementing 802.1X	288
Cracking LEAP	290
Using asleep	291
Using THC-LEAPcracker	292
Using anwrap	293
Network Authentication Countermeasures	293
WPA improves the 8021.1 picture	293

Using WPA2	294
Using a VPN	295
WIDS	296
Use the right EAP	297
Setting up a WDMZ	297
Using the Auditor Collection	297

***Part IV: The Part of Tens*301**

Chapter 16: Ten Essential Tools for Hacking Wireless Networks303

Laptop Computer	303
Wireless Network Card	304
Antennas and Connecting Cables	304
GPS Receiver	304
Stumbling Software	304
Wireless Network Analyzer	305
Port Scanner	305
Vulnerability Assessment Tool	305
Google	305
An 802.11 Reference Guide	305

Chapter 17: Ten Wireless Security-Testing Mistakes307

Skipping the Planning Process	307
Not Involving Others in Testing	308
Not Using a Methodology	308
Forgetting to Unbind the NIC When Wardriving	309
Failing to Get Written Permission to Test	312
Failing to Equip Yourself with the Proper Tools	313
Over-Penetrating Live Networks	314
Using Data Improperly	314
Failing to Report Results or Follow Up	314
Breaking the Law	316

Chapter 18: Ten Tips for Following Up after Your Testing321

Organize and Prioritize Your Results	321
Prepare a Professional Report	322
Retest If Necessary	322
Obtain Sign-Off	322
Plug the Holes You Find	323
Document the Lessons Learned	323
Repeat Your Tests	323
Monitor Your Airwaves	324
Practice Using Your Wireless Tools	324
Keep Up with Wireless Security Issues	324

Part V: Appendixes	325
Appendix A: Wireless Hacking Resources	327
Certifications	327
General Resources	327
Hacker Stuff	328
Wireless Organizations	328
Institute of Electrical and Electronics Engineers (IEEE): www.ieee.org	328
Wi-Fi Alliance (formerly WECA): www.wifialliance.com	329
Local Wireless Groups	329
Security Awareness and Training	331
Wireless Tools	331
General tools	331
Vulnerability databases	332
Linux distributions	332
Software emulators	333
RF prediction software	333
RF monitoring	333
Antennae	335
Wardriving	335
Wireless IDS/IPS vendors	336
Wireless sniffers	337
WEP/WPA cracking	338
Cracking passwords	338
Dictionary files and word lists	339
Gathering IP addresses and SSIDs	339
LEAP crackers	340
Network mapping	340
Network scanners	340
Appendix B: Glossary of Acronyms	341
Index	347