
Contents

Foreword	xiii
Authors.....	xv
1 Hacking Windows OS.....	1
Introduction	1
Physical Access.....	2
Live CDs	3
Just Burned My First ISO.....	4
Before You Start.....	6
Utility Manager.....	8
Sticky Keys	15
How to Log In without Knowing the Password.....	21
Using Kon-Boot to Get into Windows without a Password	24
Bart's PE and WindowsGate.....	26
Old School.....	29
2000 Server Family Domain Controllers.....	30
Defending against Physical Attacks on Windows Machines	31
Partitioning Your Drive for BitLocker	32
Windows 7	32
Windows Vista	32
Trusted Platform Modules.....	33
Using BitLocker with a TPM	34
Using BitLocker without a TPM	34
Windows 7	35
Vista and 2008	38
BitLocker Hacks.....	39
TrueCrypt	39
Evil Maid.....	43
Summary	45
2 Obtaining Windows Passwords	47
Introduction	47
Ophcrack.....	48

Password Hashes.....	50
Nediam.com.mx.....	51
John the Ripper.....	51
Rainbow Tables.....	54
Cain & Abel.....	57
Helix.....	71
Switchblade.....	77
Countermeasures.....	86
Summary.....	87
3 Imaging and Extraction	89
Introduction	89
Computer Forensic Tools.....	90
Imaging with FTK Imager	90
Live View.....	93
Deleted Files and Slack Space	99
Forensic Tool Kit.....	100
Imaging with Linux dd.....	103
Understanding How Linux Recognizes Devices	103
Creating a Forensic Image	107
Imaging over a Network.....	111
Examining an Image	114
Autopsy	115
Conclusion.....	117
4 Bypassing Web Filters	119
Introduction	119
Information You Provide.....	120
Changing Information.....	120
Summary.....	131
5 Manipulating the Web	133
Introduction	133
Change the Price with Tamper Data.....	133
Paros Proxy.....	138
Firebug	143
SQL Injection.....	144
Cross-Site Scripting	146
Countermeasures	148
Parameterized Statements	149
Validating Inputs.....	149
Escaping Characters	149
Filtering Characters and Statements	149
Encryption.....	149
Account Privileges	149
Errors.....	150
Further Resources and References.....	150

6	Finding It All on the Net	151
	Introduction	151
	Before You Start.....	152
	Researching with Caution.....	155
	RapidShare	157
	Advanced Google.....	162
	YouTube.....	163
	News Servers.....	166
	BitTorrent	167
	Other Options	167
	ShodanHQ.com.....	171
7	Research Time	179
	Overview	179
	Research, Time, and Planning.....	180
	All Vectors Possible	180
	Internal or External Intelligence	181
	Direct Contact versus Indirect Contact	181
	Learning the Topology.....	182
	Learning the Structure.....	183
	Techniques and Tools	184
	Whois	184
	Reserved Addresses	184
	How to Defend	186
	Domain Dossier: Central Ops	187
	Defense against Cyber Squatters.....	189
	DNS Records.....	189
	Traceroute.....	190
	Commands to Perform a Command Line Traceroute.....	192
	Traceroute: Central Ops	192
	Traceroute: Interpretation of DNS.....	193
	Disable Unused Services	195
	Domain Check: Central Ops.....	195
	Email Dossier: Central Ops.....	195
	Site Report: Netcraft.com	196
	Wayback Machine: Archive.org	198
	How to Defend against This.....	199
	Whois History: DomainTools.org.....	199
	Zone-h.org.....	200
	Indirect Web Browsing and Crawling.....	200
	Indirect Research: Google.com	201
	Google Search Commands	201
	How to Defend against This.....	202
	Indirect Recon: Cache, Google.com	202
	Indirect Research: Google Hacking Database.....	203
	Indirect Research: lmgty.com	203
	Indirect Research: Duckduckgo.com	204
	Summary	204

8	Capturing Network Traffic.....	205
	Overview	205
	Network Placement.....	206
	Collision Domains.....	206
	Intrusion Detection at the Packet Level	207
	Monitoring Limitations	207
	Network Response Methodology.....	208
	Monitoring/Capturing.....	208
	Viewing Text Data.....	209
	Searching Text and Binary.....	209
	Filtering	210
	Windows Executable and Signatures.....	211
	Common File Signatures of Malware.....	211
	Snort.....	212
	Snort Rules	212
	Making a Snort Rule	213
	Sample Content Fields	213
	Analysis	213
	Capture Information.....	213
	Capinfos	214
	Setting Up Wireshark	214
	Coloring Rules.....	214
	Filtering Data in Wireshark	215
	Wireshark Important Filters	215
	Wireshark Operators.....	216
	Wireshark Filters.....	216
	Packet Options	217
	Following the Stream.....	218
	Wireshark Statistics	218
	Network Extraction	219
	Summary	221
9	Research Time: Finding the Vulnerabilities.....	223
	Overview	223
	Methodology	223
	Stealth.....	224
	Offensive Security's Exploit Database	225
	CVEs.....	226
	Security Bulletins	226
	Zero Day Exploits.....	227
	Security Focus	227
	Shellcode.....	229
	Running Shellcode	229
	BackTrack.....	230
	BackTrack Tools	230
	BackTrack Scanning	231
	Windows Emulation in BackTrack	231

Wine.....	231
A Table for Wine Commands.....	232
Information Gathering and Vulnerability Assessment Using BackTrack.....	232
Maltego.....	232
Nmap.....	233
Zenmap.....	233
Nmap Scanning for Subnet Ranges (Identifying Hosts).....	235
Nmap Scanning for Subnet Ranges (Identifying Services).....	236
Nmap Scanning for Subnet Ranges (Identifying Versions).....	237
Nmap Scanning Firewall/IDS Evasion.....	238
Nmap Scanning Decoys.....	239
Nmap Randomization and Speed.....	240
PortQry.....	241
Autoscan.....	241
Nessus.....	241
Upgrade the Vulnerability/Plug-ins Database.....	242
Nessus Policies.....	243
Nessus Credentials.....	243
OpenVAS.....	245
Plug-in Update.....	246
Netcat.....	248
Port Scanning with Netcat.....	248
Nikto.....	250
Summary.....	251
10 Metasploit.....	253
Introduction.....	253
Payload into EXE.....	271
WebDAV DLL Hijacker.....	283
Summary.....	287
11 Other Attack Tools.....	289
Overview.....	289
Sysinternals.....	289
Pslist.....	289
Tasklist/m.....	290
Netstat -ano.....	290
Process Explorer.....	291
Remote Administration Tools.....	291
Poison Ivy RAT.....	292
Accepting Poison Ivy Connections.....	292
Building Poison Ivy Backdoors.....	293
Preparing Beaconsing Malware.....	293
Preparing Install of Malware.....	294
Advanced Poison Ivy Options.....	295
Generating a PE.....	296
Commanding and Controlling Victims with Poison Ivy.....	296

Statistics.....	297
Command and Control	297
Information	298
Management.....	298
Files	298
Processes	299
Tools.....	299
Active Ports.....	300
Password Audit	300
Surveillance	301
Shark	301
To Create a Server.....	301
Startup.....	302
Binding.....	302
Blacklist.....	303
Stealth.....	303
Antidebugging.....	304
Compile.....	304
Compile Summary.....	305
Command and Control with Shark	306
File Searching	307
Printer.....	308
Summary	308
12 Social Engineering with Web 2.0	309
Introduction	309
People Search Engines	317
A Case Study	324
Summary.....	328
13 Hack the Macs	329
Introduction	329
Mac OS X and Safari 5 Internet Artifacts.....	339
FileVault	343
FileVault Security Concerns.....	345
TrueCrypt	346
iPhone	350
Summary.....	357
14 Wireless Hacking	359
Introduction	359
Wi-Fi Hardware and Software.....	360
BackTrack Setup: Quick and Dirty	360
Monitor Mode	361
Cracking WPA-PSK	362
Wired Equivalent Privacy Cracking.....	365
Wi-Fi Monitoring and Capturing	366

Physical Wi-Fi Device Identification.....	370
WPA Rainbow Tables.....	371
Analyzing Wi-Fi Network Traffic	373
Network Analysis	373
Example Scenario: “Man in the Middle”	380
Summary.....	388
Index	391