

Contents

Foreword	.xxiii
Chapter 1 Google Searching Basics	1
Introduction	2
Exploring Google's Web-Based Interface	2
Google's Web Search Page	2
Google Web Results Page	5
Google Groups	6
Google Image Search	8
Google Preferences	9
Language Tools	12
Building Google Queries	14
The Golden Rules of Google Searching	14
Basic Searching	17
Using Boolean Operators and Special Characters	18
Search Reduction	21
Working With Google URLs	24
URL Syntax	25
Special Characters	26
Putting the Pieces Together	27
Summary	37
Solutions Fast Track	37
Links to Sites	38
Frequently Asked Questions	39
Chapter 2 Advanced Operators	41
Introduction	42
Operator Syntax	43
Troubleshooting Your Syntax	44

Introducing Google's Advanced Operators	46
Intitle and Allintitle: Search Within the Title of a Page	46
Allintext: Locate a String Within the Text of a Page	49
Inurl and Allinurl: Finding Text in a URL	50
Site: Narrow Search to Specific Sites	52
Filetype: Search for Files of a Specific Type	54
Link: Search for Links to a Page	59
Inanchor: Locate Text Within Link Text	62
Cache: Show the Cached Version of a Page	62
Numrange: Search for a Number	63
Daterange: Search for Pages Published Within a Certain Date Range	64
Info: Show Google's Summary Information	65
Related: Show Related Sites	66
Author: Search Groups for an Author of a Newsgroup Post	66
Group: Search Group Titles	69
Insubject: Search Google Groups Subject Lines	69
Msgid: Locate a Group Post by Message ID	70
Stocks: Search for Stock Information	71
Define: Show the Definition of a term	72
Phonebook: Search Phone Listings	72
Colliding Operators and Bad Search-Fu	75
Summary	80
Solutions Fast Track	80
Links to Sites	85
Frequently Asked Questions	85
Chapter 3 Google Hacking Basics	87
Introduction	88
Anonymity with Caches	88
Using Google as a Proxy Server	95
Directory Listings	99
Locating Directory Listings	100
Finding Specific Directories	101
Finding Specific Files	102
Server Versioning	103

Going Out on a Limb: Traversal Techniques	108
Directory Traversal	109
Incremental Substitution	110
Extension Walking	111
Summary	115
Solutions Fast Track	115
Links to Sites	118
Frequently Asked Questions	118
Chapter 4 Preassessment	121
Introduction	122
The Birds and the Bees	122
Intranets and Human Resources	123
Help Desks	124
Self-Help and “How-To” Guides	124
Job Listings	126
Long Walks on the Beach	126
Names, Names, Names	127
Automated E-Mail Trolling	128
Addresses, Addresses, and More Addresses!	134
Nonobvious E-Mail Relationships	139
Personal Web Pages and Blogs	140
Instant Messaging	140
Web-Based Mailing Lists	141
Résumés and Other Personal Information	142
Romantic Candlelit Dinners	143
Badges? We Don’t Need No Steenkin’ Badges!	143
What’s Nearby?	143
Coffee Shops	144
Diners and Delis	144
Gas Stations	145
Bars and Nightclubs	145
Preassessment Checklist	146
Summary	147
Solutions Fast Track	147
Links to Sites	148
Frequently Asked Questions	148

Chapter 5 Network Mapping	151
Introduction	152
Mapping Methodology	152
Mapping Techniques	154
Domain Determination	154
Site Crawling	155
Page Scraping Domain Names	156
API Approach	158
Link Mapping	159
Group Tracing	164
Non-Google Web Utilities	166
Targeting Web-Enabled Network Devices	171
Locating Various Network Reports	173
Summary	176
Solutions Fast Track	176
Links to Sites	177
Frequently Asked Questions	178
Chapter 6 Locating Exploits and Finding Targets	181
Introduction	182
Locating Exploit Code	182
Locating Public Exploit Sites	182
Locating Exploits Via Common Code Strings	184
Locating Vulnerable Targets	186
Locating Targets Via Demonstration Pages	187
Locating Targets Via Source Code	189
Locating Targets Via CGI Scanning	197
Summary	200
Solutions Fast Track	200
Links to Sites	201
Frequently Asked Questions	201
Chapter 7 Ten Simple Security Searches That Work	203
Introduction	204
site	204
intitle:index.of	206
error warning	206

login logon	208
username userid employee.ID “your username is”	209
password passcode “your password is”	210
admin administrator	210
–ext:html –ext:htm –ext:shtml –ext:asp –ext:php	212
inurl:temp inurl:tmp inurl:backup inurl:bak	216
intranet help.desk	216
Summary	218
Solutions Fast Track	218
Frequently Asked Questions	220
Chapter 8 Tracking Down Web Servers, Login Portals, and Network Hardware	221
Introduction	222
Locating and Profiling Web Servers	223
Directory Listings	223
Web Server Software Error Messages	225
Microsoft Internet Information Server (IIS)	225
Apache Web Server	229
Application Software Error Messages	238
Default Pages	241
Default Documentation	246
Sample Programs	248
Locating Login Portals	250
Locating Network Hardware	255
Summary	259
Solutions Fast Track	259
Frequently Asked Questions	261
Chapter 9 Usernames, Passwords, and Secret Stuff, Oh My!	263
Introduction	264
Searching for Usernames	264
Searching for Passwords	270
Searching for Credit Card Numbers, Social Security Numbers, and More	276
Social Security Numbers	279
Personal Financial Data	279

Searching for Other Juicy Info	.280
Summary	.285
Solutions Fast Track	.285
Frequently Asked Questions	.287

Chapter 10 Document Grinding and Database Digging .289

Introduction	.290
Configuration Files	.291
Log Files	.297
Office Documents	.299
Database Digging	.301
Login Portals	.302
Support Files	.304
Error Messages	.306
Database Dumps	.309
Actual Database Files	.310
Automated Grinding	.312
Google Desktop Search	.316
Summary	.317
Solutions Fast Track	.317
Links to Sites	.318
Frequently Asked Questions	.319

Chapter 11 Protecting Yourself from Google Hackers 321

Introduction	.322
A Good, Solid Security Policy	.322
Web Server Safeguards	.323
Directory Listings and Missing Index Files	.324
Blocking Crawlers with Robots.txt	.325
NOARCHIVE: The Cache “Killer”	.327
NOSNIPPET: Getting Rid of Snippets	.327
Password-Protection Mechanisms	.328
Software Default Settings and Programs	.330
Hacking Your Own Site	.331
Site Yourself	.332
Gooscan	.332
Installing Gooscan	.333

Gooscan's Options	334
Gooscan's Data Files	335
Using Gooscan	338
Windows Tools and the .NET Framework	342
Athena	343
Using Athena's Config Files	345
Constructing Athena Config Files	346
The Google API and License Keys	348
SiteDigger	348
Wikto	351
Getting Help from Google	354
Summary	358
Solutions Fast Track	358
Links to Sites	359
Frequently Asked Questions	360
Chapter 12 Automating Google Searches	363
Introduction	364
Understanding Google Search Criteria	365
Analyzing the Business Requirements for Black Hat Auto-Googling	368
Google Terms and Conditions	368
Understanding the Google API	369
Understanding a Google Search Request	371
Auto-Googling the Google Way	375
Google API Search Requests	375
Reading Google API Results Responses	376
Sample API Code	377
Source Documentation	381
Understanding Google Attack Libraries	384
Pseudocoding	385
Perl Implementation	386
Source Documentation	389
Python Implementation	390
Source	391
Output	392
Source Documentation	392

C# Implementation (.NET)	393
Source Documentation	396
C Implementation	397
Source Documentation	405
Scanning the Web with Google Attack Libraries	406
CGI Vulnerability Scanning	406
Output	411
Summary	412
Solutions Fast Track	412
Links to Sites	413
Frequently Asked Questions	414
Appendix A Professional Security Testing	417
Introduction	418
Professional Security Testing	419
The Open Methodology	420
The Standardized Methodology	423
Connecting the Dots	429
Summary	434
Links to Sites	434
Mailing Lists	434
Frequently Asked Questions	435
Appendix B An Introduction to Web	
 Application Security	437
Introduction	438
Defining Web Application Security	438
The Uniqueness of Web Application Security	439
Web Application Vulnerabilities	440
Constraints of Search-Engine Hacking	443
Information and Vulnerabilities in Content	445
The Fast Road to Directory Enumerations	445
Robots.txt	445
FTP Log Files	446
Web Traffic Reports	447
HTML Comments	447
Error Messages	448
Sample Files	449

Bad Extensions	.449
System Documentation	.452
Hidden Form Fields, JavaScript, and Other	
Client-Side Issues	.453
Playing with Packets	.453
Viewing and Manipulating Packets	.456
Code Vulnerabilities in Web Applications	.459
Client-Side Attacks	.459
Escaping from Literal Expressions	.463
Session Hijacking	.468
Command Execution: SQL Injection	.471
Enumerating Databases	.475
Summary	.478
References	.478
Solutions Fast Track	.479
Frequently Asked Questions	.482

Appendix C Google Hacking Database

A number of extended tables and additional penetration testing tools are accessible from the Syngress Solutions Site (www.syngress.com/solutions).

Index	.485
--------------	-------------