

Contents

Chapter 1 Reconnaissance	1
Objectives	2
Approach	4
A Methodology for Reconnaissance	5
Intelligence Gathering	6
Footprinting	16
Verification	23
Core Technologies	33
Intelligence Gathering	33
Search Engines	33
WHOIS	34
RWHOIS	35
Domain Name Registries and Registrars	35
Web Site Copiers	36
Social Networking Services	37
Footprinting	37
DNS	38
SMTP	41
Verification	42
Virtual Hosting	43
IP Subnetting	43
The Regional Internet Registries	43
Open Source Tools	46
Intelligence Gathering Tools	46
Web Resources	47
Linux/UNIX Command-Line Tools	51
Open Source Windows Tools	62
Footprinting Tools	66
Web Resources	67
Linux/UNIX Console Tools	68
Open Source Windows Tools	70
Verification Tools	72
Web Resources	72
Linux/UNIX Console Tools	76

Case Study: The Tools in Action82
 Intelligence Gathering, Footprinting, and Verification of an
 Internet-Connected Network.82
 Footprinting.93
 Verification.94

Chapter 2 Enumeration and Scanning 99

Introduction100
Objectives.100
 Before You Start100
 Why Do This?.101
Approach102
 Scanning.102
 Enumeration103
 Notes and Documentation103
 Active versus Passive104
 Moving On104
Core Technology.104
 How Scanning Works105
 Port Scanning.106
 Going behind the Scenes with Enumeration.107
 Service Identification108
 RPC Enumeration108
 Fingerprinting109
 Being Loud, Quiet, and All That Lies Between109
 Timing.110
 Bandwidth Issues110
 Unusual Packet Formation110
Open Source Tools111
 Scanning.111
 Nmap.111
 Netenum: Ping Sweep.119
 Unicornscan: Port Scan and Fuzzing120
 Scanrand: Port Scan.121
 Enumeration123
 Nmap: Banner Grabbing123
 Netcat123
 P0f: Passive OS Fingerprinting.126
 Xprobe2: OS Fingerprinting126
 Httpprint128

Ike-scan:VPN Assessment	129
Amap: Application Version Detection	130
Windows Enumeration: Smbgetserverinfo/smbdumppusers/smbclient.	131
Nbtscan	134
Smb-nat: Windows/Samba SMB Session Brute Force	134
Case Studies: The Tools in Action.	136
External	136
Internal.	138
Stealthy.	143
Noisy (IDS) Testing	146
Further Information	148
Chapter 3 Hacking Database Services.	153
Introduction	154
Objectives.	154
Approach	154
Core Technologies.	154
Basic Terminology	155
Database Installation	156
Default Users and New Users	157
Roles and Privileges	160
Technical Details.	162
Case Studies: Using Open Source and Closed Source Tools.	164
Microsoft SQL Server	164
Discovering Microsoft SQL Servers	164
Identifying Vulnerable Microsoft SQL Server Services.	168
Attacking Microsoft SQL Server Authentication.	174
Microsoft SQL Server Password Creation Guidelines	175
Microsoft SQL Default Usernames and Passwords	175
Creating Username and Dictionary Files	177
SQL Auditing Tools (SQLAT)	177
Obtaining and Cracking Microsoft SQL Server Password Hashes	179
Analyzing the Database	184
Obtaining Access to the Host Operating System.	186
SQLAT: SQLExec (Sqlquery), TFTP, and fgdump.exe	189
Oracle Database Management System.	192
Identifying and Enumerating Oracle Database with Nmap	193
Penetration Testing Oracle Services with BackTrack	200
Cracking Oracle Database Hashes	208
Privilege Escalation in Oracle from TNS Listener, No Password	214

SQL Clients	217
Shell Usage and History	217
Arguments Viewable by All Users.	218
History and Trace Logs	218
Further Information	218
Chapter 4 Web Server and Web Application Testing	221
Objectives.	222
Introduction	222
Web Server Vulnerabilities: A Short History.	222
Web Applications: The New Challenge.	223
Chapter Scope.	223
Approach	224
Web Server Testing	225
CGI and Default Pages Testing	226
Web Application Testing.	227
Core Technologies.	227
Web Server Exploit Basics	227
What Are We Talking About?.	227
CGI and Default Page Exploitation	232
Web Application Assessment.	234
Information Gathering Attacks	235
File System and Directory Traversal Attacks	235
Command Execution Attacks	235
Database Query Injection Attacks	235
Cross-site Scripting Attacks	236
Impersonation Attacks.	236
Parameter Passing Attacks	237
Open Source Tools	237
Intelligence Gathering Tools.	237
Scanning Tools.	246
Assessment Tools	258
Authentication	262
Proxy	274
Exploitation Tools	277
Metasploit	277
SQL Injection Tools	280
Case Studies: The Tools in Action.	288
Web Server Assessments	288
CGI and Default Page Exploitation	293
Web Application Assessment.	302

Chapter 5 Wireless Penetration Testing Using BackTrack 2	323
Introduction	324
Approach	325
Understanding WLAN Vulnerabilities	325
Evolution of WLAN Vulnerabilities.	326
Core Technologies.	328
WLAN Discovery	328
Choosing the Right Antenna.	330
WLAN Encryption	331
No Encryption.	331
Wired Equivalent Privacy (WEP).	332
Wi-Fi Protected Access (WPA/WPA2)	332
Extensible Authentication Protocol (EAP)	332
Virtual Private Network (VPN).	333
WLAN Attacks	333
Attacks against WEP	333
Attacks against WPA	335
Attacks against LEAP	335
Attacks against VPN	335
Open Source Tools	336
Information Gathering Tools	336
Google (Internet Search Engines)	337
WiGLE.net (Work Smarter, Not Harder)	337
Usenet Newsgroups	337
Scanning Tools.	338
Kismet	338
Footprinting Tools	342
Enumeration Tools.	343
Vulnerability Assessment Tools	344
Exploitation Tools	346
MAC Address Spoofing.	347
Deauthentication with Aireplay-ng	348
Cracking WEP with the Aircrack-ng Suite	349
Cracking WPA with CoWPAtty	359
Bluetooth Vulnerabilities	362
Bluetooth Discovery	363
Exploiting Bluetooth Vulnerabilities	364
The Future of Bluetooth.	365
Case Studies	366
Case Study: Cracking WEP	366

Case Study: Cracking WPA-PSK368
Case Study: Exploiting Bluetooth.....370
Summary372

Chapter 6 Network Devices 373

Objectives.....374
Approach374
Core Technologies.....375
Open Source Tools376
 Footprinting Tools.....376
 Traceroute376
 DNS376
 Nmap.....378
 ICMP379
 ike-scan380
 Scanning Tools.....382
 Nmap.....382
 ASS386
 Cisco Torch387
 Enumeration Tools.....389
 SNMP389
 Finger389
 Vulnerability Assessment Tools390
 Nessus390
 Exploitation Tools391
 onesixtyone391
 Hydra.....392
 TFTP Brute Force394
 Cisco Global Exploiter395
 Internet Routing Protocol Attack
 Suite (IRPAS)397
 Ettercap399
Case Study: The Tools in Action.....400
 Obtaining a Router Configuration by Brute Force401
 Where to Go from Here?408
Further Information409
 Common and Default Vendor Passwords.....412
 Modification of cge.pl413
 References413
 Software414

Chapter 7 Customizing BackTrack 2	415
Introduction	416
Module Management	416
Locating Modules	416
Converting Modules from Different Formats	418
Creating a Module from Source	419
Adding Modules to Your BackTrack Live CD or HD Installation	419
Hard Drive Installation	421
Basic Hard Drive Installation	421
Dual Boot Installation (Windows XP and BackTrack)	423
Other Configurations	426
USB Installation	426
USB Thumb Drive Installation	426
The Easiest Way to Install BackTrack to a USB Thumb Drive Using Windows	427
Alternative Directions to Install BackTrack on a USB Thumb Drive Using Windows	429
Installing BackTrack on a USB Thumb Drive Using Linux	433
Saving a USB Configuration	434
Directions to Save Your Changes on Your BackTrack USB Thumb Drive	434
Directions to Save Your New Changes (and Keep Your Old Ones) on Your BackTrack USB Thumb Drive	435
Directions to Write a Script to Save Your New Changes (and Keep Your Old Ones) on Your BackTrack USB Thumb Drive	435
External USB Hard Drive Installation	436
Installing Additional Open Source Tools	443
Updating Scripts	443
Installing aircrack-ptw	445
Installing Nessus	446
Installing Metasploit Framework 3.0 GUI	449
Installing VMWare Server	450
Installing Java for Firefox	451
Further Information	451
Quick Reference to Other Customizations	452
Remote-Exploit Forums and BackTrack Wiki	452
Credits	453
Chapter 8 Forensic Discovery and Analysis Using Backtrack	455
Introduction	456
Digital Forensics	458

- Acquiring Images 458
 - Linux dd 460
 - Linux dcfldd 470
 - dd_rescue 473
- Forensic Analysis 474
 - Autopsy 475
 - mboxgrep 478
 - memfetch 480
 - Memfetch Find 483
 - pasco. 485
 - Rootkit Hunter. 487
 - The Sleuth Kit 489
 - The Sleuth Kit Continued: Allin1 for
The Sleuth Kit. 494
 - Vinetto 498
- File Carving 500
 - Foremost. 503
 - Magicrescue 504
- Case Studies: Digital Forensics with the Backtrack Distribution. 507
- Summary 518
- Chapter 9 Building Penetration Test Labs. 519**
 - Introduction 520
 - Setting Up a Penetration Test Lab 520
 - Safety First 520
 - Isolating the Network 521
 - Concealing the Network Configuration. 522
 - Securing Install Disks 523
 - Transferring Data 525
 - Labeling 526
 - Destruction and Sanitization 526
 - Reports of Findings 527
 - Final Word on Safety. 529
 - Types of Pen-Test Labs. 529
 - The Virtual Pen-Test Lab. 529
 - The Internal Pen-Test Lab. 530
 - The External Pen-Test Lab 531
 - The Project-Specific Pen-Test Lab. 532
 - The Ad Hoc Lab 532
 - Selecting the Right Hardware 533
 - Focus on the “Most Common” 533

Use What Your Clients Use534

Dual-Use Equipment534

Selecting the Right Software535

 Open Source Tools535

 Commercial Tools536

Running Your Lab.537

 Managing the Team537

 Team “Champion”537

 Project Manager537

 Training and Cross-Training538

 Metrics.539

 Selecting a Pen-Test Framework.540

 OSSTMM540

 NIST SP 800-42.541

 ISSAF.542

Targets in the Penetration Test Lab543

 Foundstone543

 De-ICE.net.544

 What Is a LiveCD?544

 Advantages of Pen-test LiveCDs545

 Disadvantages of Pen-test LiveCDs545

Building a LiveCD Scenario.546

 Difficulty Levels546

 Real-World Scenarios547

 Creating a Background Story548

 Adding Content548

 Final Comments on LiveCDs549

Using a LiveCD in a Penetration Test Lab.549

 Scenario549

 Network Setup.550

 Open Source Tools550

Other Scenario Ideas553

 Old Operating System Distributions553

 Vulnerable Applications554

 Capture the Flag Events554

What’s Next?.555

 Forensics.555

 Training555

Summary557

Index 559