

Contents

| | |
|--|--------------|
| Foreword | xxvii |
| Chapter 1 Reconnaissance | 1 |
| Objectives | 2 |
| Approach | 5 |
| A Methodology for Reconnaissance | 5 |
| Intelligence Gathering | 7 |
| Footprinting | 19 |
| Verification | 25 |
| Core Technologies | 35 |
| Intelligence Gathering | 35 |
| Search Engines | 36 |
| WHOIS | 37 |
| RWHOIS | 38 |
| Domain Name Registries and Registrars | 38 |
| Web Site Copiers | 40 |
| Footprinting | 40 |
| DNS | 40 |
| SMTP | 44 |
| Verification | 46 |
| Virtual Hosting | 46 |
| IP Subnetting | 47 |
| The Regional Internet Registries | 47 |
| Open Source Tools | 50 |
| Intelligence-Gathering Tools | 50 |
| Web Resources | 51 |
| *nix Command-Line Tools | 55 |
| Open Source Windows Tools | 65 |
| WinBiLE (www.sensepost.com/research) | 66 |

| | |
|--|-----------|
| Footprinting Tools | 67 |
| Web Resources | 68 |
| *nix Console Tools | 69 |
| Open Source Windows Tools | 72 |
| Verification Tools | 73 |
| Web Resources | 74 |
| *nix Console Tools | 77 |
| Case Studies—The Tools in Action | 80 |
| Intelligence Gathering, Footprinting, and Verification of an Internet-Connected Network | 81 |
| Footprinting | 88 |
| Verification | 90 |
| Chapter 2 Enumeration and Scanning | 95 |
| Objectives | 96 |
| Approach | 97 |
| Scanning | 97 |
| Enumeration | 98 |
| Core Technology | 100 |
| How Scanning Works | 100 |
| Port Scanning | 101 |
| Going Behind the Scenes with Enumeration | 105 |
| Service Identification | 105 |
| RPC Enumeration | 106 |
| Fingerprinting | 106 |
| Being Loud, Quiet, and All that Lies Between | 106 |
| Timing | 107 |
| Bandwidth Issues | 107 |
| Unusual Packet Formation | 108 |
| Open Source Tools | 108 |
| Scanning | 108 |
| Fyodor's nmap | 108 |
| netenum: Ping Sweep | 115 |
| unicornscan: Port Scan | 116 |
| scanrand: Port Scan | 117 |
| Enumeration | 119 |
| nmap: Banner Grabbing | 119 |

| | |
|---|------------|
| Windows Enumeration: smbgetserverinfo/ smbdumppusers | 125 |
| Case Studies—The Tools in Action | 131 |
| External | 131 |
| Internal | 136 |
| Stealthy | 140 |
| Noisy (IDS Testing) | 143 |
| Further Information | 146 |
| Chapter 3 Introduction to Testing Databases | 149 |
| Objectives | 150 |
| Intended Audience | 150 |
| Introduction | 151 |
| Approach | 151 |
| Context of Database Assessment | 152 |
| Process of Penetration Testing a Database | 152 |
| Core Technologies | 153 |
| Basic Terminology | 153 |
| Database Installation | 155 |
| Default Users and New Users | 156 |
| Roles and Privileges | 158 |
| Technical Details | 161 |
| Open Source Tools | 163 |
| Intelligence Gathering | 163 |
| Footprinting, Scanning, and Enumeration Tools | 164 |
| Locating Database Servers by Port | 164 |
| Enumeration Tools | 166 |
| Unauthenticated Enumeration | 166 |
| Vulnerability Assessment and Exploit Tools | 174 |
| Nessus Checks | 174 |
| Interpreting Nessus Database Vulnerabilities | 174 |
| OScanner and OAT | 176 |
| SQLAT | 177 |
| WHAX Tools | 178 |
| Case Studies—The Tools in Action | 179 |
| MS SQL Assessment | 180 |
| Oracle Assessment | 183 |

| | |
|---|------------|
| Further Information | 188 |
| Discovering Databases | 188 |
| Enumeration Tools | 188 |
| Chapter 4 Web Server & Web Application Testing | 189 |
| Objectives | 190 |
| Introduction | 190 |
| Web Server Vulnerabilities—A Short History | 190 |
| Web Applications—The New Challenge | 191 |
| Chapter Scope | 192 |
| Approach | 192 |
| Approach: Web Server Testing | 193 |
| Approach: CGI and Default Pages Testing | 195 |
| Approach: Web Application Testing | 196 |
| Core Technologies | 196 |
| Web Server Exploit Basics | 196 |
| What Are We Talking About? | 196 |
| CGI and Default Page Exploitation | 202 |
| Web Application Assessment | 204 |
| Information Gathering Attacks | 205 |
| File System and Directory Traversal Attacks | 205 |
| Command Execution Attacks | 205 |
| Database Query Injection Attacks | 206 |
| Cross-site Scripting | 207 |
| Authentication and Authorization | 207 |
| Parameter Passing Attacks | 207 |
| Open Source Tools | 208 |
| Intelligence Gathering Tools | 208 |
| Scanning Tools | 217 |
| Assessment Tools | 229 |
| Authentication | 231 |
| Proxy | 242 |
| Exploitation Tools | 245 |
| Case Studies—The Tools in Action | 248 |
| Web Server Assessments | 248 |
| CGI and Default Page Exploitation | 254 |
| Web Application Assessment | 263 |

Chapter 5 Wireless Penetration Testing Using Auditor 277

| | |
|--|-----|
| Objectives | 278 |
| Introduction | 278 |
| Approach | 279 |
| Understanding WLAN Vulnerabilities | 279 |
| Evolution of WLAN Vulnerabilities | 280 |
| Core Technologies | 281 |
| WLAN Discovery | 282 |
| Choosing the Right Antenna | 283 |
| WLAN Encryption | 284 |
| Wired Equivalent Privacy (WEP) | 284 |
| WiFi Protected Access (WPA/WPA2) | 285 |
| Extensible Authentication Protocol (EAP) | 285 |
| Virtual Private Network (VPN) | 286 |
| Attacks | 286 |
| Attacks Against WEP | 286 |
| Attacks Against WPA | 288 |
| Attacks Against LEAP | 289 |
| Attacks Against VPN | 289 |
| Open Source Tools | 290 |
| Footprinting Tools | 290 |
| Intelligence Gathering Tools | 291 |
| USENET Newsgroups | 292 |
| Google (Internet Search Engines) | 292 |
| Scanning Tools | 293 |
| Wellenreiter | 293 |
| Kismet | 295 |
| Enumeration Tools | 298 |
| Vulnerability Assessment Tools | 299 |
| Exploitation Tools | 301 |
| MAC Address Spoofing | 301 |
| Deauthentication with Void11 | 302 |
| Cracking WEP with the Aircrack Suite | 303 |
| Cracking WPA with the CoWPAtty | 306 |
| Case Studies | 307 |
| Case Study—Cracking WEP | 307 |

| | |
|---|------------|
| Case Study—Cracking WPA-PSK | 311 |
| Further Information | 314 |
| Additional GPSMap Map Servers | 314 |
| Chapter 6 Network Devices | 317 |
| Objectives | 318 |
| Approach | 318 |
| Core Technologies | 319 |
| Open-Source Tools | 320 |
| Foot Printing Tools | 320 |
| Traceroute | 320 |
| DNS | 321 |
| Nmap | 322 |
| ICMP | 323 |
| Ike-scan | 324 |
| Scanning Tools | 326 |
| Nmap | 326 |
| ASS | 329 |
| Cisco Torch | 331 |
| Snmpfuzz.pl | 332 |
| Enumeration Tools | 332 |
| SNMP | 332 |
| Finger | 334 |
| Vulnerability Assessment Tools | 334 |
| Nessus | 334 |
| Exploitation Tools | 335 |
| ADMSnmp | 335 |
| Hydra | 336 |
| TFTP-Bruteforce | 338 |
| Cisco Global Exploiter | 339 |
| Internet Routing Protocol Attack Suite (IRPAS) .. | 340 |
| Ettercap | 343 |
| Case Studies—The Tools in Action | 344 |
| Obtaining a Router Configuration by Brute Force ... | 344 |
| Further Information | 353 |
| Common and Default Vendor Passwords | 355 |
| Modification of cge.pl | 356 |

| | |
|--|------------|
| References | 356 |
| Software | 357 |
| Chapter 7 Writing Open Source Security Tools | 359 |
| Introduction | 360 |
| Why Would You Want to Learn to Code? | 360 |
| The Process of Programming | 360 |
| Step 1: Solve the Right Problem by Asking the Right Questions | 361 |
| Step 2: Breaking the Problem into Smaller, Manageable Problems | 362 |
| Step 3: Write Pseudocode | 364 |
| Step 4: Implement the Actual Code | 365 |
| Languages | 365 |
| Programming Languages | 366 |
| Logo | 366 |
| BASIC | 367 |
| Delphi | 367 |
| C/C++ | 368 |
| PERL | 368 |
| C# | 369 |
| Python | 370 |
| Java | 370 |
| Web Application Languages | 371 |
| PHP | 371 |
| ASP/ASP .NET | 371 |
| Interactive Development Environments | 371 |
| Eclipse | 372 |
| KDevelop | 382 |
| Microsoft Visual Studio .NET | 388 |
| Monodevelop | 392 |
| Quick Start Mini Guides | 395 |
| PERL Mini Guide | 395 |
| Basic Program Structure, Data Structures, Conditionals, and Loops | 395 |
| Basic File IO and Subroutines | 398 |
| Writing to a Socket and Using MySQL | 401 |

xxii Contents

| | |
|--|------------|
| Consuming a Web Service and Writing a CGI | 406 |
| C# Mini Guide | 412 |
| Basic Program Structure, Data Structures, Conditionals, and Loops | 412 |
| Basic File IO and Databases | 415 |
| Writing to Sockets | 419 |
| Conclusion | 423 |
| Useful functions and code snippets | 423 |
| C# Snippets | 423 |
| PERL Code Snippets | 427 |
| Links to Resources in this Chapter / Further Reading . . . | 428 |
| Chapter 8 Nessus | 429 |
| Introduction | 430 |
| What Is It? | 430 |
| Basic Components | 431 |
| Client and Server | 431 |
| The Plugins | 434 |
| The Knowledge Base | 435 |
| Launching Nessus | 435 |
| Running Nessus from Auditor | 436 |
| Point and Click: Launching Nessus From Within Auditor | 436 |
| Behind the Scenes: Analyzing Auditor's start-nessus Script | 440 |
| From The Ground Up: Nessus Without A Startup Script | 442 |
| Running Nessus on Windows | 446 |
| Maintaining Nessus | 448 |
| Standard Plug-In Update | 448 |
| Auditor's Plug-In Update: Method #1 | 449 |
| Auditor's Plug-In Update: Method #2 | 452 |
| Updating the Nessus Program | 456 |
| Using Nessus | 457 |
| Plugins | 458 |
| Prefs (The Preferences Tab) | 459 |
| Scan Options | 464 |

| | |
|---|------------|
| Target Selection | 466 |
| Summary | 467 |
| Solutions Fast Track | 467 |
| Links to Sites | 469 |
| Frequently Asked Questions | 469 |
| Chapter 9 Coding for Nessus | 471 |
| Introduction | 472 |
| History | 472 |
| Goals of NASL | 473 |
| Simplicity and Convenience | 473 |
| Modularity and Efficiency | 473 |
| Safety | 474 |
| NASL's Limitations | 474 |
| NASL Script Syntax | 474 |
| Comments | 474 |
| Variables | 475 |
| Operators | 478 |
| Control Structures | 483 |
| Writing NASL Scripts | 487 |
| Writing Personal-Use Tools in NASL | 488 |
| Networking Functions | 488 |
| HTTP Functions | 488 |
| Packet Manipulation Functions | 488 |
| String Manipulation Functions | 489 |
| Cryptographic Functions | 489 |
| The NASL Command-Line Interpreter | 489 |
| Programming in the Nessus Framework | 491 |
| Descriptive Functions | 491 |
| Case Study: The Canonical NASL Script | 494 |
| Porting to and from NASL | 497 |
| Logic Analysis | 498 |
| Identify Logic | 498 |
| Pseudo Code | 499 |
| Porting to NASL | 500 |
| Porting to NASL from C/C++ | 501 |
| Porting from NASL | 507 |

| | |
|---|------------|
| Case Studies of Scripts | 508 |
| Microsoft IIS HTR ISAPI Extension Buffer Overflow Vulnerability | 508 |
| Case Study: IIS .HTR ISAPI Filter Applied CVE-2002-0071 | 509 |
| Microsoft IIS/Site Server codebrws.asp Arbitrary File Access | 513 |
| Case Study: Codebrws.asp Source Disclosure Vulnerability CVE-1999-0739 | 514 |
| Microsoft SQL Server Bruteforcing | 516 |
| Case Study: Microsoft's SQL Server Bruteforce | 517 |
| ActivePerl perlIIS.dll Buffer Overflow Vulnerability .. | 526 |
| Case Study: ActivePerl perlIS.dll Buffer Overflow | 527 |
| Microsoft FrontPage/IIS Cross-Site Scripting shtml.dll Vulnerability | 531 |
| Case Study: Microsoft FrontPage XSS | 531 |
| Summary | 536 |
| Solutions FastTrack | 537 |
| Links to Sites | 539 |
| Frequently Asked Questions | 540 |
| Chapter 10 NASL Extensions and Custom Tests | 543 |
| Introduction | 544 |
| Extending NASL Using Include Files | 544 |
| Include Files | 544 |
| Extending the Capabilities of Tests Using the Nessus Knowledge Base | 550 |
| Extending the Capabilities of Tests Using Process Launching and Results Analysis | 552 |
| What Can We Do with TRUSTED Functions? | 553 |
| Creating a TRUSTED Test | 554 |
| Summary | 562 |
| Chapter 11 Understanding the Extended Capabilities of the Nessus Environment | 563 |
| Introduction | 564 |

| | |
|--|------------|
| Windows Testing Functionality Provided by the smb_nt.inc Include File | .564 |
| Windows Testing Functionality Provided by the smb_hotfixes.inc Include File | .569 |
| UNIX Testing Functionality Provided by the Local Testing Include Files | .573 |
| Summary | .580 |
| Chapter 12 Extending Metasploit I | 581 |
| Introduction | .582 |
| Using the MSF | .582 |
| The msfweb Interface | .583 |
| The msfconsole Interface | .597 |
| Starting msfconsole | .597 |
| General msfconsole Commands | .598 |
| The MSF Environment | .599 |
| Exploiting with msfconsole | .604 |
| The msfcli Interface | .613 |
| Updating the MSF | .619 |
| Summary | .621 |
| Solutions Fast Track | .621 |
| Links to Sites | .621 |
| Frequently Asked Questions | .622 |
| Chapter 13 Extending Metasploit II | 625 |
| Introduction | .626 |
| Exploit Development with Metasploit | .626 |
| Determining the Attack Vector | .627 |
| Finding the Offset | .628 |
| Selecting a Control Vector | .634 |
| Finding a Return Address | .641 |
| Using the Return Address | .647 |
| Determining Bad Characters | .648 |
| Determining Space Limitations | .650 |
| Nop Sleds | .652 |
| Choosing a Payload and Encoder | .654 |
| Integrating Exploits into the Framework | .665 |

xxvi Contents

| | |
|--|------------|
| Understanding the Framework | .666 |
| Analyzing an Existing Exploit Module | .667 |
| Overwriting Methods | .673 |
| Summary | .675 |
| Solutions Fast Track | .675 |
| Links to Sites | .676 |
| Frequently Asked Questions | .677 |
| Index. | 679 |