## Contents

Acknowledgments ........................................................................................................................................ xxi
Foreword ................................................................................................................................................... xix

### PART 1  SETTING UP

| CHAPTER 1 | Introduction ........................................................................................................................................ 3 |
| Introduction ........................................................................................................................................ 3 |
| About the Book ................................................................................................................................. 4 |
| Target Audience ............................................................................................................................... 4 |
| How to Use This Book ...................................................................................................................... 5 |
| About the DVD .................................................................................................................................. 7 |
| Course Material ............................................................................................................................... 8 |
| Reference Material ............................................................................................................................ 8 |
| LiveCDs ................................................................................................................................................ 8 |
| Summary ............................................................................................................................................. 10 |
| Solutions Fast Track ......................................................................................................................... 10 |
| About the Book ................................................................................................................................ 10 |
| About the DVD ................................................................................................................................ 11 |
| Reference .......................................................................................................................................... 11 |

| CHAPTER 2 | Ethics and Hacking ...................................................................................................................... 13 |
| Introduction ....................................................................................................................................... 13 |
| Why Stay Ethical? ............................................................................................................................... 15 |
| Black Hat Hackers ............................................................................................................................. 15 |
| White Hat Hackers .............................................................................................................................. 17 |
| Gray Hat Hackers ............................................................................................................................... 18 |
| Ethical Standards .............................................................................................................................. 19 |
| Certifications ..................................................................................................................................... 19 |
| Contractor ......................................................................................................................................... 19 |
| Employer ........................................................................................................................................... 20 |
| Educational and Institutional Organizations .................................................................................... 21 |
| Computer Crime Laws ...................................................................................................................... 24 |
| Types of Laws .................................................................................................................................... 24 |
| Type of Computer Crimes and Attacks ............................................................................................. 24 |
| U.S. Federal Laws .............................................................................................................................. 27 |
| U.S. State Laws ................................................................................................................................. 29 |
CHAPTER 4  Setting Up Your Lab ................................................................. 101
  Introduction .................................................................................... 101
  Personal Lab .................................................................................. 102
    Keeping it Simple ......................................................................... 102
  Equipment ....................................................................................... 102
  Software .......................................................................................... 103
  Lab for Book Exercises ................................................................. 103
  Corporate Lab ................................................................................ 106
    Internal Labs ................................................................................ 107
    External Labs ............................................................................... 107
    Equipment .................................................................................... 107
    Software ........................................................................................ 108
  Protecting Penetration Test Data .................................................... 108
    Encryption Schemas .................................................................... 108
    Securing PenTest Systems ............................................................ 110
    Mobile Security Concerns ............................................................. 111
    Wireless Lab Data ........................................................................ 112
  Additional Network Hardware ......................................................... 112
    Routers ......................................................................................... 113
    Firewalls ........................................................................................ 113
    Intrusion Detection System/Intrusion Prevention System .............. 114
  Summary .......................................................................................... 114
  Solutions Fast Track ....................................................................... 115
    Personal Lab ................................................................................. 115
    Corporate Lab ............................................................................... 115
    Protecting Penetration Test Data .................................................. 115
    Additional Network Hardware ....................................................... 115
  Frequently Asked Questions ............................................................ 116
  Expand Your Skills .......................................................................... 116
  Reference .......................................................................................... 117

CHAPTER 5  Creating and Using PenTest Targets in Your Lab ............... 119
  Introduction .................................................................................... 119
  Turn-Key Scenarios versus Real-World Targets ............................... 120
    Problems with Learning to Hack .................................................... 120
    Real-World Scenarios ................................................................. 121
  Turn-Key Scenarios ....................................................................... 122
    What is a LiveCD? ........................................................................ 123
    De-ICE ......................................................................................... 123
    Hackerdemia ................................................................................. 127
CHAPTER 6 Methodologies .......................................................... 153
Introduction .............................................................................. 153
Project Management Body of Knowledge .............................. 154
   Introduction to PMBOK ......................................................... 155
   Initiating Process Group ...................................................... 155
   Planning Process Group ...................................................... 157
   Executing Process Group .................................................... 161
   Closing Process Group ....................................................... 163
   Monitoring and Controlling Process Group ......................... 163
Information System Security Assessment Framework .............. 166
   Planning and Preparation – Phase I ..................................... 166
   Assessment – Phase II ........................................................ 166
   Reporting, Clean-up, and Destroy Artifacts – Phase III .......... 170
Open Source Security Testing Methodology Manual ............... 171
   Rules of Engagement ........................................................ 172
   Channels ............................................................................ 173
   Modules ............................................................................. 175
Summary .................................................................................. 176
CHAPTER 7 PenTest Metrics .................................................. 181
    Introduction ............................................................. 181
    Quantitative, Qualitative, and Mixed Methods ................. 182
        Quantitative Analysis ............................................. 182
        Qualitative Analysis ............................................ 183
        Mixed Method Analysis ......................................... 185
    Current Methodologies .............................................. 186
        Project Management Institute ................................. 186
        ISSAF .................................................................... 191
        OSSTMM ................................................................ 192
        Tool-Generated Reports ........................................... 193
    Summary ..................................................................... 194
    Solutions Fast Track ................................................. 195
        Quantitative, Qualitative, and Mixed Methods ............. 195
        Current Methodologies .......................................... 195
    Frequently Asked Questions ........................................... 196
    References .................................................................. 196

CHAPTER 8 Management of a PenTest .................................... 197
    Introduction ............................................................. 197
    Project Team Members ................................................. 197
        Roles and Responsibilities ........................................ 198
        Organizational Structure ......................................... 202
    Project Management .................................................. 206
        Initiating Stage ...................................................... 206
        Planning Stage ....................................................... 208
        Executing Stage ..................................................... 209
        Monitoring and Controlling ...................................... 211
        Closing Stage ....................................................... 211
    Summary ..................................................................... 214
    Solutions Fast Track .................................................. 214
        Project Team Members ............................................. 214
        Project Management .............................................. 214
PART 2  RUNNING A PENTEST

CHAPTER 9  Information Gathering .................................. 219
  Introduction .......................................................... 219
  Passive Information Gathering ................................... 221
    Web Presence ....................................................... 222
    Corporate Data .................................................... 231
    WHOIS and DNS Enumeration ................................. 233
    Additional Internet Resources ................................. 236
  Active Information Gathering .................................... 238
    DNS Interrogation ................................................ 238
    E-mail Accounts .................................................. 240
    Perimeter Network Identification ............................. 242
    Network Surveying ............................................... 246
  Project Management ................................................. 247
    Executing Process Phase ....................................... 248
    Monitoring and Control Process .............................. 250
  Summary ..................................................................... 253
Solutions Fast Track ...................................................... 253
  Passive Information Gathering .................................... 253
  Active Information Gathering ..................................... 254
  Project Management .................................................. 254
  Frequently Asked Questions ...................................... 254
Expand Your Skills .......................................................... 255
References .................................................................... 257

CHAPTER 10  Vulnerability Identification ............................ 259
  Introduction ............................................................. 259
  Port Scanning ............................................................ 260
    Target Verification ................................................... 261
    UDP Scanning .......................................................... 264
    TCP Scanning .......................................................... 265
    Perimeter Avoidance Scanning ................................... 268
  System Identification .................................................. 272
    Active OS Fingerprinting .......................................... 272
    Passive OS Fingerprinting ......................................... 272
CHAPTER 11 Vulnerability Verification ........................................... 285
Introduction ........................................................................... 285
Exploit Codes – Finding and Running ................................... 287
Internet Sites ......................................................................... 287
Automated Tools ................................................................... 290
Exploit Codes – Creating Your Own ....................................... 320
Fuzzing .................................................................................. 322
Code Review .......................................................................... 324
Application Reversing ............................................................ 324
Web Hacking .......................................................................... 325
SQL Injection .......................................................................... 326
Cross-Site Scripting ................................................................. 327
Web Application Vulnerabilities ............................................... 330
Project Management ............................................................... 332
Executing Process Phase ......................................................... 332
Monitoring and Control Process ............................................... 333
Summary ................................................................................ 334
Solutions Fast Track ................................................................. 335
Exploit Codes – Finding and Running ................................... 335
Exploit Codes – Creating Your Own ....................................... 335
Web Hacking .......................................................................... 335
Project Management ............................................................... 335
Frequently Asked Questions .................................................. 336
Expand Your Skills ................................................................. 336
References .............................................................................. 338
CHAPTER 12 Compromising a System and Privilege Escalation

Introduction ......................................................... 339
System Enumeration .................................................. 341
  Internal Vulnerabilities ........................................ 341
  Sensitive Data .................................................... 347
Network Packet Sniffing ............................................ 348
Social Engineering .................................................... 354
  Baiting ............................................................... 355
  Phishing ............................................................. 355
  Pretexting ......................................................... 355
Wireless Attacks ...................................................... 356
  Wi-Fi Protected Access Attack ................................ 357
  WEP Attack ......................................................... 362
Project Management .................................................. 364
  Executing Process Phase ....................................... 364
  Monitoring and Control Process ................................. 365
Summary ............................................................. 365
Solutions Fast Track .................................................. 366
  System Enumeration .............................................. 366
  Network Packet Sniffing ......................................... 367
  Social Engineering ............................................... 367
  Wireless Attacks .................................................. 367
  Project Management ............................................. 367
Frequently Asked Questions ...................................... 368
Expand Your Skills ................................................... 368
References ............................................................ 369

CHAPTER 13 Maintaining Access

Introduction .......................................................... 371
Shells and Reverse Shells ............................................. 372
  Netcat Shell ........................................................ 372
  Netcat Reverse Shell ............................................. 376
Encrypted Tunnels ..................................................... 379
  Adding a Host Firewall (Optional) ............................... 380
  Setting Up the SSH Reverse Shell ................................. 381
Other Encryption and Tunnel Methods ............................. 386
Summary ............................................................. 387
Solutions Fast Track .................................................. 388
  Shells and Reverse Shells ........................................ 388
  Encrypted Tunnels ............................................... 388
  Other Encryption and Tunnel Methods ........................... 388