# Contents

*Introduction*  
*Assessment Test*  

## Chapter 1  
**Introduction to Ethical Hacking**  
1  
Hacking: the Evolution  
   The Early Days of Hacking  
   Current Developments  
   Hacking: Fun or Criminal Activity?  
   The Evolution and Growth of Hacking  
So, What Is an Ethical Hacker?  
   What Are Your Responsibilities?  
   Code of Conduct and Ethics  
   Ethical Hacking and Penetration Testing  
   Hacking Methodologies  
   Vulnerability Research and Tools  
   What Is Incident Response?  
   Business Continuity Plan  
   Ethics and the Law  
Summary  
Exam Essentials  
Review Questions  

## Chapter 2  
**System Fundamentals**  
39  
Exploring Network Topologies  
Working with the Open Systems Interconnection Model  
Dissecting the TCP/IP Suite  
IP Subnetting  
Hexadecimal vs. Binary  
Exploring TCP/IP Ports  
   Domain Name System  
Understanding Network Devices  
   Routers and Switches  
Working with MAC Addresses  
   Proxies and Firewalls  
Intrusion Prevention and Intrusion Detection Systems  
Network Security  
Knowing Operating Systems  
   Microsoft Windows  
   Mac OS
Android 62
Linux 62
Backups and Archiving 63
Summary 64
Exam Essentials 65
Review Questions 66

Chapter 3  Cryptography 71
Cryptography: Early Applications and Examples 73
  History of Cryptography 73
  Tracing the Evolution 75
Cryptography in Action 76
  So How Does It Work? 77
  Symmetric Cryptography 77
  Asymmetric, or Public Key, Cryptography 80
Understanding Hashing 86
Issues with Cryptography 88
Applications of Cryptography 89
  IPsec 90
  Pretty Good Privacy 92
  Secure Sockets Layer 93
Summary 94
Exam Essentials 94
Review Questions 95

Chapter 4  Footprinting 99
Understanding the Steps of Ethical Hacking 100
  Phase 1: Footprinting 100
  Phase 2: Scanning 101
  Phase 3: Enumeration 101
  Phase 4: System Hacking 102
What Is Footprinting? 102
  Why Perform Footprinting? 103
  Goals of the Footprinting Process 103
Terminology in Footprinting 106
  Open Source and Passive Information Gathering 106
  Passive Information Gathering 106
  Pseudonymous Footprinting 106
  Internet Footprinting 107
Threats Introduced by Footprinting 107
The Footprinting Process 108
  Using Search Engines 108
  Google Hacking 108
<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Scanning</th>
<th>127</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is Scanning?</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Types of Scans</td>
<td>129</td>
<td></td>
</tr>
<tr>
<td>Checking for Live Systems</td>
<td>130</td>
<td></td>
</tr>
<tr>
<td>Wardialing</td>
<td>131</td>
<td></td>
</tr>
<tr>
<td>Using Ping</td>
<td>133</td>
<td></td>
</tr>
<tr>
<td>Hping3: the Heavy Artillery</td>
<td>134</td>
<td></td>
</tr>
<tr>
<td>Checking the Status of Ports</td>
<td>135</td>
<td></td>
</tr>
<tr>
<td>The Family Tree of Scans</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>Full-Open Scan</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>Stealth or Half-Open Scan</td>
<td>138</td>
<td></td>
</tr>
<tr>
<td>Xmas Tree Scan</td>
<td>139</td>
<td></td>
</tr>
<tr>
<td>FIN Scan</td>
<td>140</td>
<td></td>
</tr>
<tr>
<td>NULL Scan</td>
<td>141</td>
<td></td>
</tr>
<tr>
<td>Idle Scanning</td>
<td>142</td>
<td></td>
</tr>
<tr>
<td>ACK Scanning</td>
<td>143</td>
<td></td>
</tr>
<tr>
<td>UDP Scanning</td>
<td>144</td>
<td></td>
</tr>
<tr>
<td>OS Fingerprinting</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>Active Fingerprinting with Nmap</td>
<td>146</td>
<td></td>
</tr>
<tr>
<td>Passive Fingerprinting an OS</td>
<td>147</td>
<td></td>
</tr>
<tr>
<td>Banner Grabbing</td>
<td>149</td>
<td></td>
</tr>
<tr>
<td>Countermeasures</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Scanning</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td>Mapping the Network</td>
<td>152</td>
<td></td>
</tr>
<tr>
<td>Using Proxies</td>
<td>153</td>
<td></td>
</tr>
<tr>
<td>Setting a Web Browser to Use a Proxy</td>
<td>154</td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>Exam Essentials</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>Review Questions</td>
<td>156</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6  Enumeration

A Quick Review 160
Footprinting 160
Scanning 161
What Is Enumeration? 161
About Windows Enumeration 163
Users 163
Groups 164
Security Identifiers 166
Linux Basic 168
Users 168
Services and Ports of Interest 169
Commonly Exploited Services 170
NULL Sessions 173
SuperScan 174
DNS Zone Transfers 174
The PsTools Suite 177
Using finger 178
Enumeration with SNMP 178
Management Information Base 179
SNScan 180
Unix and Linux Enumeration 180
finger 180
rpcinfo 181
showmount 181
enum4linux 181
LDAP and Directory Service Enumeration 182
JXplorer 183
Preventing LDAP Enumeration 183
Enumeration Using NTP 184
SMTP Enumeration 184
Using VRFY 185
Using EXPN 185
Using RCPT TO 186
SMTP Relay 186
Summary 187
Exam Essentials 187
Review Questions 189

Chapter 7  System Hacking

Up to This Point 194
Footprinting 194
Scanning 195
Enumeration 195
Chapter 8  Malware  223

Malware  224
  Malware and the Law  226
  Categories of Malware  227
  Viruses  228
  Worms  234
  Spyware  236
  Adware  237
  Scareware  237
  Ransomware  238
  Trojans  238

Overt and Covert Channels  247

Summary  249

Exam Essentials  250

Review Questions  251

Chapter 9  Sniffers  255

Understanding Sniffers  256

Using a Sniffer  259
  Sniffing Tools  259
  Wireshark  260
  Tcpdump  264
  Reading Sniffer Output  266

Switched Network Sniffing  270
  MAC Flooding  270
  ARP Poisoning  271
  MAC Spoofing  272
  Port Mirror or SPAN Port  272
  On the Defensive  273
  Mitigating MAC Flooding  274
  Detecting Sniffing Attacks  275

Summary  275

Exam Essentials  276

Review Questions  277
# Contents

**Chapter 10 Social Engineering**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is Social Engineering?</td>
<td>282</td>
</tr>
<tr>
<td>Why Does Social Engineering Work?</td>
<td>283</td>
</tr>
<tr>
<td>The Power of Social Engineering</td>
<td>284</td>
</tr>
<tr>
<td>Social-Engineering Phases</td>
<td>285</td>
</tr>
<tr>
<td>What Is the Impact of Social Engineering?</td>
<td>285</td>
</tr>
<tr>
<td>Common Targets of Social Engineering</td>
<td>286</td>
</tr>
<tr>
<td>Social Networking to Gather Information?</td>
<td>287</td>
</tr>
<tr>
<td>Networking</td>
<td>289</td>
</tr>
<tr>
<td>Countermeasures for Social Networking</td>
<td>291</td>
</tr>
<tr>
<td>Commonly Employed Threats</td>
<td>293</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>296</td>
</tr>
<tr>
<td>Protective Measures</td>
<td>297</td>
</tr>
<tr>
<td>Know What Information Is Available</td>
<td>298</td>
</tr>
<tr>
<td>Summary</td>
<td>298</td>
</tr>
<tr>
<td>Exam Essentials</td>
<td>299</td>
</tr>
<tr>
<td>Review Questions</td>
<td>300</td>
</tr>
</tbody>
</table>

**Chapter 11 Denial of Service**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding DoS</td>
<td>306</td>
</tr>
<tr>
<td>DoS Targets</td>
<td>308</td>
</tr>
<tr>
<td>Types of Attacks</td>
<td>308</td>
</tr>
<tr>
<td>Buffer Overflow</td>
<td>314</td>
</tr>
<tr>
<td>Understanding DDoS</td>
<td>317</td>
</tr>
<tr>
<td>DDoS Attacks</td>
<td>318</td>
</tr>
<tr>
<td>DoS Tools</td>
<td>319</td>
</tr>
<tr>
<td>DDoS Tools</td>
<td>320</td>
</tr>
<tr>
<td>DoS Defensive Strategies</td>
<td>323</td>
</tr>
<tr>
<td>Botnet-Specific Defenses</td>
<td>323</td>
</tr>
<tr>
<td>DoS Pen-Testing Considerations</td>
<td>324</td>
</tr>
<tr>
<td>Summary</td>
<td>324</td>
</tr>
<tr>
<td>Exam Essentials</td>
<td>324</td>
</tr>
<tr>
<td>Review Questions</td>
<td>326</td>
</tr>
</tbody>
</table>

**Chapter 12 Session Hijacking**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Session Hijacking</td>
<td>332</td>
</tr>
<tr>
<td>Spoofing vs. Hijacking</td>
<td>334</td>
</tr>
<tr>
<td>Active and Passive Attacks</td>
<td>335</td>
</tr>
<tr>
<td>Session Hijacking and Web Apps</td>
<td>336</td>
</tr>
<tr>
<td>Types of Application-Level Session Hijacking</td>
<td>337</td>
</tr>
<tr>
<td>A Few Key Concepts</td>
<td>341</td>
</tr>
<tr>
<td>Network Session Hijacking</td>
<td>344</td>
</tr>
</tbody>
</table>
Chapter 13 Web Servers and Applications

Chapter 14 SQL Injection

Chapter 15 Hacking Wi-Fi and Bluetooth
Summary 433
Exam Essentials 434
Review Questions 435

Chapter 16 Mobile Device Security 439

Mobile OS Models and Architectures 440
Goals of Mobile Security 441
Device Security Models 442
  Google Android OS 443
  Apple iOS 446
  Common Problems with Mobile Devices 447
  Penetration Testing Mobile Devices 449
  Penetration Testing Using Android 450
Countermeasures 454
Summary 455
Exam Essentials 456
Review Questions 457

Chapter 17 Evasion 461

Honeypots, IDSs, and Firewalls 462
  The Role of Intrusion Detection Systems 462
  Firewalls 467
  What’s That Firewall Running? 470
  Honeypots 473
  Run Silent, Run Deep: Evasion Techniques 475
  Evading Firewalls 477
Summary 480
Exam Essentials 481
Review Questions 482

Chapter 18 Cloud Technologies and Security 485

What Is the Cloud? 486
  Types of Cloud Solutions 487
  Forms of Cloud Services 488
  Threats to Cloud Security 489
  Cloud Computing Attacks 491
  Controls for Cloud Security 494
  Testing Security in the Cloud 495
Summary 496
Exam Essentials 497
Review Questions 498
Chapter 19  Physical Security  501

Introducing Physical Security  502
Simple Controls  503
Dealing with Mobile Device Issues  505
Data Storage Security  506
Securing the Physical Area  510
Entryways  517
Server Rooms and Networks  518
Other Items to Consider  519
Education and Awareness  519
Defense in Depth  519
Summary  520
Exam Essentials  521
Review Questions  522

Appendix A  Answers to Review Questions  525

Chapter 1: Introduction to Ethical Hacking  526
Chapter 2: System Fundamentals  527
Chapter 3: Cryptography  528
Chapter 4: Footprinting  529
Chapter 5: Scanning  530
Chapter 6: Enumeration  532
Chapter 7: System Hacking  532
Chapter 8: Malware  533
Chapter 9: Sniffers  534
Chapter 10: Social Engineering  536
Chapter 11: Denial of Service  537
Chapter 12: Session Hijacking  539
Chapter 13: Web Servers and Applications  540
Chapter 14: SQL Injection  541
Chapter 15: Hacking Wi-Fi and Bluetooth  542
Chapter 16: Mobile Device Security  544
Chapter 17: Evasion  544
Chapter 18: Cloud Technologies and Security  546
Chapter 19: Physical Security  547

Appendix B  Penetration Testing Frameworks  549

Overview of Alternative Methods  550
Penetration Testing Execution Standard  552
Working with PTES  553
Pre-Engagement Interactions  553
Appendix C Building a Lab

Why Build a Lab? 566
  The Build Process 566
  What You Will Need 567
Creating a Test Setup 568
  Virtualization Software Options 569
The Installation Process 569
  Installing a Virtualized Operating System 570
  Installing Tools 570
Summary 574

Index 575