<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td></td>
<td>xxiii</td>
</tr>
<tr>
<td><strong>Chapter 1</strong> x86 and x64</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Register Set and Data Types</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Instruction Set</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Syntax</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Data Movement</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td><strong>Exercise</strong></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Arithmetic Operations</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Stack Operations and Function Invocation</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td><strong>Exercises</strong></td>
<td></td>
<td>17</td>
</tr>
<tr>
<td>Control Flow</td>
<td></td>
<td>17</td>
</tr>
<tr>
<td><strong>System Mechanism</strong></td>
<td></td>
<td>25</td>
</tr>
<tr>
<td>Address Translation</td>
<td></td>
<td>26</td>
</tr>
<tr>
<td>Interrupts and Exceptions</td>
<td></td>
<td>27</td>
</tr>
<tr>
<td><strong>Walk-Through</strong></td>
<td></td>
<td>28</td>
</tr>
<tr>
<td><strong>Exercises</strong></td>
<td></td>
<td>35</td>
</tr>
<tr>
<td><strong>x64</strong></td>
<td></td>
<td>36</td>
</tr>
<tr>
<td>Register Set and Data Types</td>
<td></td>
<td>36</td>
</tr>
<tr>
<td>Data Movement</td>
<td></td>
<td>36</td>
</tr>
<tr>
<td>Canonical Address</td>
<td></td>
<td>37</td>
</tr>
<tr>
<td>Function Invocation</td>
<td></td>
<td>37</td>
</tr>
<tr>
<td><strong>Exercises</strong></td>
<td></td>
<td>38</td>
</tr>
<tr>
<td><strong>Chapter 2</strong> ARM</td>
<td></td>
<td>39</td>
</tr>
<tr>
<td>Basic Features</td>
<td></td>
<td>40</td>
</tr>
<tr>
<td>Data Types and Registers</td>
<td></td>
<td>43</td>
</tr>
<tr>
<td>System-Level Controls and Settings</td>
<td></td>
<td>45</td>
</tr>
<tr>
<td>Introduction to the Instruction Set</td>
<td></td>
<td>46</td>
</tr>
</tbody>
</table>
Loading and Storing Data 47
  LDR and STR 47
  Other Usage for LDR 51
  LDM and STM 52
  PUSH and POP 56
Functions and Function Invocation 57
Arithmetic Operations 60
Branching and Conditional Execution 61
  Thumb State 64
  Switch-Case 65
Miscellaneous 67
  Just-in-Time and Self-Modifying Code 67
  Synchronization Primitives 67
  System Services and Mechanisms 68
  Instructions 70
Walk-Through 71
Next Steps 77
Exercises 78

Chapter 3  The Windows Kernel 87
Windows Fundamentals 88
  Memory Layout 88
  Processor Initialization 89
  System Calls 92
  Interrupt Request Level 104
  Pool Memory 106
  Memory Descriptor Lists 106
  Processes and Threads 107
  Execution Context 109
  Kernel Synchronization Primitives 110
Lists 111
  Implementation Details 112
  Walk-Through 119
  Exercises 123
Asynchronous and Ad-Hoc Execution 128
  System Threads 128
  Work Items 129
  Asynchronous Procedure Calls 131
  Deferred Procedure Calls 135
  Timers 140
  Process and Thread Callbacks 142
  Completion Routines 143
I/O Request Packets 144
Structure of a Driver 146
  Entry Points 147
  Driver and Device Objects 149
IRP Handling 150
A Common Mechanism for User-Kernel Communication 150
Miscellaneous System Mechanisms 153
Walk-Throughs 155
An x86 Rootkit 156
An x64 Rootkit 172
Next Steps 178
Exercises 180
Building Confidence and Solidifying Your Knowledge 180
Investigating and Extending Your Knowledge 182
Analysis of Real-Life Drivers 184

Chapter 4 Debugging and Automation 187
The Debugging Tools and Basic Commands 188
Setting the Symbol Path 189
Debugger Windows 189
Evaluating Expressions 190
Process Control and Debug Events 194
Registers, Memory, and Symbols 198
Breakpoints 208
Inspecting Processes and Modules 211
Miscellaneous Commands 214
Scripting with the Debugging Tools 216
Pseudo-Registers 216
Aliases 219
Language 226
Script Files 240
Using Scripts Like Functions 244
Example Debug Scripts 249
Using the SDK 257
Concepts 258
Writing Debugging Tools Extensions 262
Useful Extensions, Tools, and Resources 264

Chapter 5 Obfuscation 267
A Survey of Obfuscation Techniques 269
The Nature of Obfuscation: A Motivating Example 269
Data-Based Obfuscations 273
Control-Based Obfuscation 278
Simultaneous Control-Flow and Data-Flow Obfuscation 284
Achieving Security by Obscurity 288
A Survey of Deobfuscation Techniques 289
The Nature of Deobfuscation: Transformation Inversion 289
Deobfuscation Tools 295
Practical Deobfuscation 312
## Contents

Case Study 328
* First Impressions 328
* Analyzing Handlers Semantics 330
* Symbolic Execution 333
* Solving the Challenge 334
* Final Thoughts 336

### Exercises 336

**Appendix**  Sample Names and Corresponding SHA1 Hashes 341

**Index** 343