Unauthorised Access

Physical Penetration Testing For IT Security Teams

Wil Allsopp
Unauthorised Access
Unauthorised Access

Physical Penetration Testing For IT Security Teams

Wil Allsopp
To Nique for being herself and to my family for supporting and inspiring me.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>xi</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>xv</td>
</tr>
<tr>
<td>Foreword</td>
<td>xvii</td>
</tr>
<tr>
<td><strong>1 The Basics of Physical Penetration Testing</strong></td>
<td>1</td>
</tr>
<tr>
<td>What Do Penetration Testers Do?</td>
<td>2</td>
</tr>
<tr>
<td>Security Testing in the Real World</td>
<td>2</td>
</tr>
<tr>
<td>Legal and Procedural Issues</td>
<td>4</td>
</tr>
<tr>
<td>Know the Enemy</td>
<td>8</td>
</tr>
<tr>
<td>Engaging a Penetration Testing Team</td>
<td>9</td>
</tr>
<tr>
<td>Summary</td>
<td>10</td>
</tr>
<tr>
<td><strong>2 Planning Your Physical Penetration Tests</strong></td>
<td>11</td>
</tr>
<tr>
<td>Building the Operating Team</td>
<td>12</td>
</tr>
<tr>
<td>Project Planning and Workflow</td>
<td>15</td>
</tr>
<tr>
<td>Codes, Call Signs and Communication</td>
<td>26</td>
</tr>
<tr>
<td>Summary</td>
<td>28</td>
</tr>
<tr>
<td><strong>3 Executing Tests</strong></td>
<td>29</td>
</tr>
<tr>
<td>Common Paradigms for Conducting Tests</td>
<td>30</td>
</tr>
<tr>
<td>Conducting Site Exploration</td>
<td>31</td>
</tr>
<tr>
<td>Example Tactical Approaches</td>
<td>34</td>
</tr>
<tr>
<td>Mechanisms of Physical Security</td>
<td>36</td>
</tr>
<tr>
<td>Summary</td>
<td>50</td>
</tr>
</tbody>
</table>
# CONTENTS

4 An Introduction to Social Engineering Techniques 51
   Introduction to Guerilla Psychology 53
   Tactical Approaches to Social Engineering 61
   Summary 66

5 Lock Picking 67
   Lock Picking as a Hobby 68
   Introduction to Lock Picking 72
   Advanced Techniques 80
   Attacking Other Mechanisms 82
   Summary 86

6 Information Gathering 89
   Dumpster Diving 90
   Shoulder Surfing 99
   Collecting Photographic Intelligence 102
   Finding Information From Public Sources and the Internet 107
   Electronic Surveillance 115
   Covert Surveillance 117
   Summary 119

7 Hacking Wireless Equipment 121
   Wireless Networking Concepts 122
   Introduction to Wireless Cryptography 125
   Cracking Encryption 131
   Attacking a Wireless Client 144
   Mounting a Bluetooth Attack 150
   Summary 153

8 Gathering the Right Equipment 155
   The “Get of Jail Free” Card 155
   Photography and Surveillance Equipment 157
   Computer Equipment 159
   Wireless Equipment 160
   Global Positioning Systems 165
   Lock Picking Tools 167
   Forensics Equipment 169
   Communications Equipment 170
   Scanners 171
   Summary 175
9 Tales from the Front Line 177
   SCADA Raiders 177
   Night Vision 187
   Unauthorized Access 197
   Summary 204

10 Introducing Security Policy Concepts 207
   Physical Security 208
   Protectively Marked or Classified GDI Material 213
   Protective Markings in the Corporate World 216
   Communications Security 218
   Staff Background Checks 221
   Data Destruction 223
   Data Encryption 224
   Outsourcing Risks 225
   Incident Response Policies 226
   Summary 228

11 Counter Intelligence 229
   Understanding the Sources of Information Exposure 230
   Social Engineering Attacks 235
   Protecting Against Electronic Monitoring 239
   Securing Refuse 240
   Protecting Against Tailgating and Shoulder Surfing 241
   Performing Penetration Testing 242
   Baseline Physical Security 245
   Summary 247

Appendix A: UK Law 249
   Computer Misuse Act 249
   Human Rights Act 251
   Regulation of Investigatory Powers Act 252
   Data Protection Act 253

Appendix B: US Law 255
   Computer Fraud and Abuse Act 255
   Electronic Communications Privacy Act 256
   SOX and HIPAA 257

Appendix C: EU Law 261
   European Network and Information Security Agency 261
   Data Protection Directive 263
## CONTENTS

Appendix D: Security Clearances  \hfill 265
  Clearance Procedures in the United Kingdom  \hfill 266
  Levels of Clearance in the United Kingdom  \hfill 266
  Levels of Clearance in the United States  \hfill 268

Appendix E: Security Accreditations  \hfill 271
  Certified Information Systems Security Professional  \hfill 271
  Communication–Electronics Security Group CHECK  \hfill 272
  Global Information Assurance Certification  \hfill 274
  INFOSEC Assessment and Evaluation  \hfill 275

Index  \hfill 277
Preface

This is a book about penetration testing. There is nothing innately new about that – there are dozens of books on the subject but this one is unique. It covers in as much detail as is possible the oft overlooked art of physical penetration testing rather than, say, ethical hacking. We won’t teach you how to use port scanners or analyze source code. There are plenty of places you can learn about that and, to a certain degree, if you’re reading this book then I’m going to assume you have grounding in the subject matter anyway. The purpose of this book is twofold: to provide auditing teams with the skills and the methodology they need to conduct successful physical penetration testing and to educate those responsible for keeping attackers out of their facilities.

My personal experience in physical penetration testing began about seven years ago when, following a scoping meeting to arrange an ethical hacking engagement at a data centre in London, the client asked almost as an aside, ‘By the way, do you guys do social engineering, that sort of thing – you know try and break in and stuff?’. I responded (like any junior consultant sitting next to a senior salesman) that of course we did! As it turned out we thought about it, decided to give it a shot and . . . failed. Miserably. Not surprisingly.

My team and I were hackers, lab rats. In effect, we didn’t know the first thing about breaking into buildings or conning our way past security guards. This is a situation now facing an increasing number of ethical hacking teams who are being asked to perform physical testing. We know it needs to be done and the value is obvious, but where to begin? There are no books on the subject, at least none available to the general public (other than the dodgy ones on picking locks published by Loompanics
So I decided to fill the void and write one. It has a special emphasis on combining physical testing with information security testing simply because ethical hacking teams are most likely to be employed for this kind of work (at least in the private sector) and because ultimately it’s your information systems that are the most likely target for any attacker. However, anyone with a need to understand how physical security can fail will benefit from this book – the culmination of a number of years of experience performing all manner of penetration testing in all kinds of environments.

**Who this Book Is For**

Anyone who has an interest in penetration testing and what that entails will benefit from this book. You might have an interest in becoming a penetration tester or you might work in the industry already with an aim to learn about physical penetration testing. You might want to learn how attackers gain access to facilities and how this can be prevented or perhaps you’re considering commissioning a physical penetration test and want to learn what this involves.

This book is written for you.

**What this Book Covers**

*Unauthorized Access* discusses the lifecycle of a physical penetration test from start to finish. This starts with planning and project management and progresses through the various stages of execution. Along the way, you’ll learn the skills that are invaluable to the tester including social engineering, wireless hacking, and lock picking.

The core subjects discuss what takes place during a physical penetration test, what you can expect and how to deal with problems. Equipment necessary to carrying out a test is given its own chapter.

Chapter 9 includes case studies that draw on my own personal testing experience, which I hope will inspire you. Chapters 10 and 11 focus on protecting against intruders and corporate spies and how this relates to the cornerstone of information security; the security policy.

The appendices deal with miscellaneous subjects such as law, accreditations and security clearance.
How this Book Is Structured

The two most important chapters in this book are Chapter 2 and Chapter 3. These contain the core theory and practice of physical penetration testing. The chapters that follow it discuss in depth the skill sets you will be required to master:

- **Chapter 4** – This chapter discusses how to manipulate human nature. Social engineering is the art of the con man and probably the single most crucial set of skills you will learn. The practice of these skills is at the core of any successful operating team.

- **Chapter 5** – Generally this concerns defeating locks. This chapter assumes no previous knowledge and these skills are not difficult to master. This is a crash course.

- **Chapter 6** – Knowledge is power; the more you have the more powerful you become. This chapter covers the basics of how and where to gather information, from how to successfully leverage Internet search technologies and databases through to the physical surveillance of target staff and facilities.

- **Chapter 7** – Despite the security shortcomings of wireless networks (both 802.11x and Bluetooth) being well documented, many companies continue to deploy them. I discuss equipment, how to crack encryption and bypass other security mechanisms. I provide you shortcuts to get you up and running quickly and introduce some newer techniques for compromising wireless networks that will guarantee that if you’re using wireless in your business now, you won’t be when you finish this chapter.

- **Chapter 8** – This chapter offers an in-depth discussion of the equipment you need, where to get it and how to use it.

- **Chapter 9** – This chapter offers a few historical scenarios taken from my case history. Names have been changed to protect those who should have known better.

- **Chapter 10** – This chapter provides basic information about what a security policy should cover. If you’ve read this far and still don’t have a security policy, this chapter helps you write one.

- **Chapter 11** – This chapter covers how to minimize your exposure to information leakage, social engineering and electronic surveillance.

- **Appendix A** – This provides a legal reference useful to UK testers.

- **Appendix B** – This provides a legal reference useful to US testers.

- **Appendix C** – This provides a legal reference useful when conducting testing in the European Union.