Unauthorised Access

Physical Penetration Testing For IT Security Teams

Wil Allsopp

WILEY
A John Wiley and Sons, Ltd., Publication

Unauthorised Access

Unauthorised Access

Physical Penetration Testing For IT Security Teams

Wil Allsopp

WILEY
A John Wiley and Sons, Ltd., Publication

This edition first published 2009

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

ISBN 978-0-470-74761-2

Typeset in 10/12 Optima by Laserwords Private Limited, Chennai, India
Printed and bound in Great Britain by Bell & Bain Ltd, Glasgow

To Nique for being herself and to my family for supporting and inspiring me.

Contents

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

Unlimited). 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.

- **Appendix D** – This clarifies the differing terms used in the United States and United Kingdom.
- **Appendix E** – This tells you about the various tests you can take or the tests you want to be sure a tester has taken before hiring.

What You Need to Use this Book

I've written *Unauthorized Access* to be as accessible as possible. It's not an overly technical read and although grounding in security principles is desirable, it's not a requirement. Chapter 7 (in which the discussion focuses on compromising the security of wireless technologies) is technical from start to finish but it does not assume any previous knowledge and provides references to the requisite software and hardware as well as step by step instructions. If you have a grounding in penetration testing (or at least know what it is) so much the better but again this is not necessary.

What you need to use this book and what you need to carry out a physical penetration test are two different things (for that you should refer to Chapter 8). However, I strongly recommend you have the following:

- A modern laptop computer;
- A copy of the Backtrack 3 Live Linux Disc – available from www.remote-exploit.org;
- A Backtrack compatible wireless network card (see Chapter 8).

You may also wish to purchase a set of lock picks to practice what you learn. You should consider this to be the starting point. There is a vast array of equipment relevant to this field but you don't, by any means, need all of it.

Acknowledgements

I would like to thank my superb editing team and of course my colleagues at Madison Gurkha for giving me the time to work on this. In particular I'd like to thank, in no particular order, the following: Andrew Dalton, Frans Kollée, Pieter de Boer, Tim Hemel, Arjan de Vet, Steve Witmer, Caroline van de Wiel, Hans van de Looy, Guido van Rooij, Remco Huisman, Walter Belgers, Ward Wouts, Thijs Hodiamont, Serge van den Boom, Marnix Aarts, Jan Hendrikx, Jack Franken, Haywood Mcdowell, Rob Lockwood, Corinne Hanskamp, Willem-Jan Grootjans and Gary Mcgath.

Foreword

Kevin Mitnick

Billions of dollars are spent each year by governments and industry to secure computer networks from the prying eyes of an attacker. As a security consultant, I have done quite a few system hardening jobs where the entire focus was upon the firewalls, server configuration, application security, intrusion detection systems, and the like. Some managers completely rely on this technology and put little or no emphasis on better securing their physical perimeter.

Those employed in the computer security industry are fully aware that once physical access to networks is obtained 90% of the obstacles are removed. The attackers are aware of this too, and have demonstrated their agility in bypassing standard security measures when foiled after attempts at remotely accessing a system. In addition to those on the outside that may attempt to circumvent your controls, there are many on the inside (employees and vendors) that already have access. Adding another layer of physical security may deter both of these groups. Consultants in the security field must continually expand their skill set to accommodate the ever-changing environments and protect their client's assets. In this book Wil Allsopp has created a thorough reference for those looking to advance into the area of physical penetration testing. The book also serves as a guidebook for in-house security managers seeking to institute better policy safeguards.

Every month it seems that we are hearing in the media about large-scale attacks on corporations, the government and financial institutions. Many of these have involved physical barrier penetrations, with the most notable being a huge retailer whose credit card databases were compromised by

a group that was reportedly inside the network for more than two years undetected. It was touted by the government as the largest theft to date of credit card numbers, which was placed at over 47 million accounts. How were they able to get in? One method was to swipe a wireless barcode scanner and extract the encryption key used to communicate with the wireless access point inside a retail location. The crooks also obtained physical access to a crawlspace above the store, spliced into the Ethernet, and planted their own secret wireless router. While this describes the most brazen of attackers, don't be surprised to hear more stories like this in the future. The rapidly advancing technology side of computer security is making electronic intrusions increasingly more difficult for hackers, therefore we will see greater implementation of the physical security attack methods explained in this book, played out in tandem with a technical attack.

A few years ago I was performing a penetration test, which included a scope of testing physical security controls. The first morning I dressed in my suit and arrived in the lobby of the client's office to meet with my contact. Noticing a display of business cards at the reception desk I pocketed a few inside my coat jacket. For the next two days I remained in my car, parked close by, just watching the building and observing behaviors of those coming and going. At about 8:30 each night a janitorial service arrived at the office complex to clean the offices. I knew this was my 'in'. Armed with the business cards from the first morning, and once again outfitted in a suit, I walked up to the door and began banging on the glass. A few minutes later, one of the cleaning crew arrived to open the door. I explained that I had left my keys in my office while handing him 'my' business card; he stepped aside and waved me through.

Once I was in the building I began to search for my target's cubicle (some research was performed beforehand to narrow down the location of his cubicle). I sat at the computer, turned it on, slid a Linux Live CD into the CD-ROM drive, entered in a few commands, and grabbed the Administrator's password hash for that machine. It took only a few minutes to crack the password hash using rainbow tables. Once I had access to the computer I installed a Trojan on the system (this was the set goal), powered down the system, packed up my things and left the premises. This all occurred in about twenty minutes and the client had no idea that they had been compromised until the details were provided in the report.

Securing proprietary information is multi-faceted and can no longer be approached with by focusing on the technology alone. All potential access points must be scrutinized carefully to ensure that ingress is denied on multiple levels. In *Unauthorised Access: Physical Penetration Testing For IT Security Teams*, Allsopp addresses this concept with a relevant and pertinent outline for performing physical penetrations test by familiarizing

the would-be tester with the methodologies and tools needed to perform the test, and illustrating them with the colorful recanting of tales from his vast experience as a security consultant. These stories help to provide real-world examples of the techniques that are being used by attackers every day.

Performing physical penetration testing within your organization should not only be reserved for businesses trying to safeguard information, but can be also be applied to provide better security against theft, trespassing, and guard against industrial espionage. This book will first take you through the terminology, planning, and equipment needed to perform the test. As Allsopp reminds you in later chapters, security is only as strong as its weakest link, which is most likely to be the very people employed by the target.

Once the lingo used in testing is defined, and some of the pitfalls regarding physical layouts of facilities that may be encountered are outlined, you are introduced to a primer on social engineering, which is the practice of using deception, manipulation, and influence to persuade the target to comply with your request. Allsopp recognizes that those best versed in social engineering possess certain personality traits that make them especially adept in this type of manipulation, but attempts to provide an introduction of some basic knowledge for the inexperienced to build on because he realizes the importance of mastering this skill. This is critical, as there is rarely a compromise of security that takes place without some level of social engineering.

For those that have already conducted a physical penetration test in the past, there are several chapters that should provide a few new things for your arsenal as the subject matter switches to information gathering, lock picking and wireless technology. The chapter on lock picking is brief, but provides excellent resources to learn more on the subject as well as giving the reader an overview of the basic steps in picking a lock along with general information on various locking mechanisms and how they can be bypassed. Even if you're never picked a lock before, Chapter 7 will make you want to try.

Many might not consider wireless hacking as a 'physical' attack method, but if you consider that most wireless access points have a broadcast range of less than 300 meters without a long-range antenna, to take advantage of these devices you must place yourself within the allotted radius to compromise the target. Having in-depth knowledge of wireless devices can be used for more than just attacking them. If you can obtain physical access to cabling, a 'hard-wired' network could suddenly become a wireless one, if spliced into with a device placed in-line. Wireless technology is probably one of the most commonly misconfigured items

providing perimeter security, and if compromised, it can easily become the low-hanging fruit sought by attackers.

After you are enlightened and possess a solid understanding of executing physical penetration tests, Allsopp gathers all the techniques discussed and rolls them into detailed true-life accounts in Chapter 9. The first example describes a pen test performed on a SCADA (Supervisory Control And Data Acquisition) system. There has been an elevated awareness of terrorism since 9/11, and SCADA systems have been receiving significant media attention since they are used to monitor and control critical infrastructure processes such as power generation, life support systems, water treatment, and telecommunications. Many speculators are afraid that the power grid could be compromised in a standalone terrorist act, or use in conjunction with a symbolic attack, to reduce the response time of emergency personnel to the scene. These systems are in perpetual production and are not usually connected to the internet, so taking them offline for maintenance and upgrades is very difficult, which makes their physical security all the more important.

Allsopp's example of lax security at a power substation, unfortunately, is not limited to the UK. Often, these critical systems in many countries are left unmanned and may not be protected by anything more than a barbed-wire fence and padlocks. Sure, there may be some electronically locked doors and access gates, but as shown in prior chapters, these are easily bypassed by a determined intruder. Armed with a laptop and key information, if you can get past these controls, you are most likely going to find an unpatched system that could grant you 'keys to the kingdom'.

The infusion of the real-life stories help to clearly demonstrate the typical shortcomings due to the lack of proper procedures, employee training, and policies in place. You can employ the latest technology and implement multiple layers of defense, but if your personnel are not properly trained to spot weaknesses and then act on them, all of these precautions are rendered almost useless. Allsopp addresses concepts to provide better policy, incident response, and access control. Much of this involves classifying assets so that employees are aware of what is most important to safeguard.

While this book is aimed at security consultants looking to add physical penetration testing to their repertoires it would also be a great read for those managing security for various organizations. It would be a useful reference tool for IT/Security Managers to implement better policy and training for its employees. If you could only walk away with one thing from this book it would be the lesson to teach your employees to challenge and verify. An apology is a much easier thing to give than having to explain how you were instrumental in allowing an intruder to bypass established protocols.

1

The Basics of Physical Penetration Testing

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

Sun Tzu: The Art of War

There is an old saying that security is only as strong as the weakest link in the chain. This is an erudite and often overlooked truth. The weakest link is never the cryptographic keys protecting a VPN link or the corporate firewalls guarding the borders of a network, although these technologies certainly have their shortfalls. The weakest link in any security scenario is people. Some people are lazy and all people make mistakes and can be manipulated. This is the most important security lesson you will ever learn: security in any form always boils down to people and trust. Any decent computer hacker will tell you: if you want to be good, learn technologies and programming languages, reverse engineer operating systems, and so on. To be a *great* hacker requires learning skills that are generally not maintained by people of this mindset. Once you master the manipulation of people, you can break into anything – any system whether corporate, electronic or human is vulnerable.

This chapter covers the basics of penetration testing, the things you need to know before you dive into the more interesting practical chapters. This includes a guide to terminology unique to penetration testers, a little on legal and procedural issues (because an understanding of the relevant legislation is critical) and, of course, a discussion of why penetration testing is important, including a look at what organizations usually hope to achieve from engaging in a penetration test.

Conducting physical penetration tests is a unique and challenging way to earn a living; it requires a certain mindset, a broad skill set and takes experience to become accomplished. This book can't help you with the

mindset: that's something you have to develop; or the experience: that's something you have to accumulate; but it will go a long way to providing you with the relevant skill set and this chapter is the first step.

If you are representing an organization and want to ensure that you have the highest form of security in place, penetration testing can help you. This chapter tells you what to expect from a penetration testing team.

What Do Penetration Testers Do?

Penetration testers are hired by organizations to compromise security in order to demonstrate vulnerability. They do this every day and their ability to pay the rent depends on their success at breaking through security.

To demonstrate computer security flaws, penetration testers use reverse engineering software. They hack into networks and defeat protocols. With respect to physical security, they demonstrate vulnerability through physical intrusion into client premises. This is most often achieved through covert intelligence gathering, general deception, and social engineering although it may involve a more direct approach such as a night-time intrusion, defeating locks and crawling up fire escapes, depending on the rules of engagement. The differences between computer and physical intrusion may seem vast, but there is significant crossover between the two and they are often performed in tandem.

I have been conducting penetration tests in one form or another for over a decade and in that time I've seen client requirements change – both with the changing face of technology and a growing awareness of the threats faced by organizations wishing to keep their confidential data secure. The problem in a nutshell is this: you can have the best firewalls and change control procedures; you can have regular electronic penetration testing against networks and applications; you can audit your source code and lock down your servers. All of these approaches are fine and, if conducted well, are generally worthwhile. However, if an attacker can physically penetrate your premises and access information systems directly, these strategies won't protect you. This 'hard shell, soft center' approach to security has led to some of the most serious information system breaches in memory. As you will learn, there is far more to security than SSL and patching against the latest buffer overflows.

Security Testing in the Real World

Military organizations, particularly the US military, have employed penetration testing teams (called 'tiger teams' or 'red teams') for decades.

Their remit is to penetrate friendly bases to assess the difficulty an enemy would have gaining the same access. This could involve planting a cardboard box with the word 'bomb' written on it or attempting to steal code books. It might involve gaining access to a secure location and taking photographs or taking something of intelligence value. As time has gone by, the term 'tiger team' has become more associated with computer penetration teams; however the term is still widely used in its original context within the military. The challenges faced by testers in the private and government sectors are very different from those presented to military tiger teams, not least because they have significantly less chance of being shot at. (I speak from experience . . . .) However while the attackers that one wishes to guard against are fundamentally different (terrorists in one case and industrial espionage actors in the other, for example) the approach is not dissimilar. All testers start with a specific goal, gather intelligence on their target, formulate a plan of attack based on available information and finally execute the plan. Each of these steps is covered in detail in this book but first, in the interests of consistency, let's consider some of the terms I will be using throughout this text:

- **Target** – the client initiating the test and the physical location at which the target resides;
- **Goal** – that which must be attained in order for the penetration test to be considered successful, such as the following examples:
  - Breach border security at the target location (the simplest form of test, often as basic as penetrating beyond reception, where most physical security procedures end).
  - Gain physical access to the computer network from within the target location.
  - Photograph a predetermined asset.
  - Acquire a predetermined asset.
  - Gain access to predetermined personnel.
  - Acquire predetermined intelligence on assets or personnel.
  - Plant physical evidence of presence.
  - Any combination of the above.
- **Asset** – a location within the target, something tangible the operating team must acquire (such as a server room or a document) or something intangible such as a predetermined level of access;
- **Penetration test** – a method of evaluating the security of a computer system, network or physical facility by simulating an attack by an intruder;
- **Operating team** – the team tasked with conducting a penetration test. In the context of a physical penetration and starting from the moment the test is initiated, the operating team is likely to consist of:

  - planners;
  - operators (those actually conducting the physical test);
  - support staff.
    The makeup of the team will depend on the nature of the test. For example, a test involving computer access following a successful physical penetration must have at least one operator skilled in computer intrusion. Those skilled in social engineering are likely to be deployed in a planning or support capacity.
- **Scope** – the agreed rules of engagement, usually based around a black box (zero knowledge) approach or a crystal box (information about the target is provided by the client) approach;
- **Anticipated resistance or security posture** – the resistance an operating team faces, depending on a number of factors:
  - the nature of the target;
  - security awareness among staff;
  - quantity (and quality) of security personnel;
  - general preparedness and awareness of potential threats at the target.

Other factors include the difficulty of the assignment and the effectiveness of the security mechanisms to protect assets.

Legal and Procedural Issues

International law applicable to security testing is covered in Appendices A and B. However, this overview should at least get you thinking about the legal issues you need to take into consideration.

Most clients expect – and rightly so – a penetration team to be insured before they even consider hiring them. Although I'm not going to point you in the direction of any particular insurance providers, you must possess errors and omissions coverage, at a minimum. The coverage required varies from region to region and is governed by rules laid out in specific jurisdictions.

Indemnity insurance is highly recommended. Insurance companies may want to know a little about your team members before signing off a policy. Such information could include medical backgrounds and almost certainly will include details of criminal offences (i.e. they expect to find none) as well as professional histories. None of this should be a concern because you performed background vetting on your team prior to hiring them. (Didn't you?)

When hiring a penetration testing team, be sure they are insured. This will help ensure that necessary background tests have been performed on the team you hire to access what could be private information.

Security Clearances

When performing penetration tests of any kind for either central government or the military, team members need to hold security clearances. The following information is specific to the United Kingdom although the gist is the same for the United States, where clearance procedures are far more stringent and make extensive use of polygraphs ('lie detector' tests).

> Despite overwhelming evidence to the contrary, the US government insists that polygraphs can't be beaten. They can and regularly are.

Security clearances come in different flavors depending on the nature of the work being performed and the sensitivity of the target. All clearances have to be sponsored by the department initiating the test unless they are already held by the operating team (though there are exceptions to this). In general, all testing team members are expected to hold security check (SC) clearance. Almost anyone who has no criminal record and is not known to the intelligence agencies is unlikely to be turned down for this clearance. Potential team members are required to supply basic information about themselves, including places they've lived and past employment. They are generally asked questions about their membership of organizations as well. SC clearance permits access to protectively marked (classified) information on a project-by-project, need-to-know basis (usually up to SECRET). Although this clearance must be periodically renewed, it is not (usually) necessary to clear team members for individual tests. In general, SC clearance is adequate and the most realistic choice given the lead time needed to arrange clearances.

One step up is developed vetting (DV) clearance. This is needed to work for intelligence organizations such as GCHQ or MI6 and is a minimum requirement for those regularly working at a TOP SECRET level. These clearances are issued on a project-by-project basis and they are not transferable. To obtain DV clearance, prospective applicants are required to attend an interview (usually conducted by the Defense Vetting Agency or MI5). The process includes in-depth analysis of the personal and financial background of the applicant. Family and partners are also likely to be interviewed and their responses cross-referenced. Processing DV

clearances is a costly and time-consuming business for the government and often people being vetted for government jobs start working in their new positions (albeit at a lower level of security) long before they are cleared. Only the most sensitive tests will require DV clearance.

The bottom line is to know who you are hiring so that insurance and security clearances are a mere headache rather than a major pain. In the UK, a potential hire can provide a statement from the police that no file is held on them (the Data Protection Act gives the right to such a statement).

If you are putting a penetration testing team together, I recommend that you also run a financial background check on everyone, if only to be able to show your clients that you've taken due diligence, rather than because it has any intrinsic value.

Appendix D covers security clearances in the United Kingdom and the United States.

Staying Within the Law

It should go without saying that a lot of the skills outlined in this book are of use to criminals as well as to legitimate penetration testers. I have no particular concerns in putting these skills down on paper. The bad guys are already well versed in them. However I would be remiss if I didn't point out that it is *your* responsibility to ensure you always remain on the right side of the law. As I discuss the various subjects in this book, I do my best to apprise you of any relevant legal issues you may run into but I'm not a lawyer. Your company should always obtain qualified legal advice. The following pieces of UK legislation are illustrative examples of aspects of the law you might not have considered.

Human Rights Act 1998

In 2000, the United Kingdom incorporated the European Convention on Human Rights into UK law. The majority of the Human Rights Act 1998 is irrelevant to penetration testing. However, there are one or two things to be aware of when conducting any form of penetration testing.

Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The key to Article 8 is privacy which can be (and has been) interpreted in some unexpected ways. For example, if a penetration testing team, in the execution of their duties, accidentally or deliberately intercepted the private communications of target staff, an offence has been committed under Article 8. For example, a target user checks her Yahoo! email on a company computer over the company network. Nobody has the right to intercept that email. The fact that what she's doing may be a disciplinary matter under the terms of her employment is irrelevant.

I'll give you another (true) example so that you can appreciate the scope of what I'm talking about. A hacker breaches the security of a central government department, or so he believes. Actually, he's breached a 'honey pot' set up to study hacker behavior. The hacker routes his traffic via this honey pot and uses it to check his email. In doing so, he allows his communications to be intercepted by government security personnel. This email is private; by capturing, storing (and indeed reading) the email, an offence has been committed.

The bottom line – whether you think this is crazy or not – is that you need to be aware of what you're looking at and the potential legal ramifications of what you do. If you are hiring a penetration testing team, you need to be aware of what they can legally do.

Computer Misuse Act 1990

At its core, the Computer Misuse Act 1990 makes it a crime to knowingly access an information system without permission. Read and craft your rules of engagement carefully: a penetration testing team may have permission to target a specific computer or network within the target, but not the ones adjacent to it. They may be authorized to attack a specific server, but not the applications running on it (which may be under a completely different sphere of organizational responsibility).

At any time, if the operating team is in doubt as to their legal position they should immediately confer with their support staff. See the appendices for the relevant text of US, UK and EU legislation.

Know the Enemy

I began this chapter with perhaps the most famous quotation from Sun Tzu's *Art of War*: Know the enemy and know yourself. Before you can know the enemy, you have to know who the enemy is. For the military this is straightforward: they tend to be the guys shooting at you and bombing you. In the commercial world, the enemy is not quite so simple to define. The threats that organizations face in the modern world tend to be various and multilateral.

For a physical penetration test to have any intrinsic value, it is vital to determine and, to a certain degree, emulate the nature of the threat facing that organization. The threats faced may differ dramatically. Table 1.1 briefly explains the targets and their potential exposure that operating teams are most likely to encounter. This subject gets much more detailed treatment later in the book. The given threat should not necessarily alter your approach, but it should certainly guide it.

Table 1.1 Targets and threats

Targets	Potential threats
Corporate targets (headquarters; larger self-contained facilities)	Breached border security: wide-ranging access
Corporate offices (shared premises), usually managed by building services or a central reception	Breached border security: easy to breach, corporate espionage
Data centers (third-party facilities for data storage)	Attractive targets across the board
Local government or council offices	Journalists and protesters
Central government offices	Foreign intelligence, protesters and activists
Police headquarters	Organized crime, activists and journalists
Utilities	Terrorism
Power stations	Terrorism
Military bases	Foreign intelligence and protesters

There is a certain degree of crossover. For example, a corporate defense contractor can be considered as a military target. How these threats manifest themselves varies: