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:

- **Commercial espionage** – This can involve external hacking, physical intrusion into corporate premises, use of moles or sleepers to gather confidential information, etc.
- **Commercial sabotage** – Such acts can and have included 'ethical' or 'environmental' terrorism i.e. attacks on facilities owned by drug companies, oil companies, animal testing facilities or abortion clinics (the latter being largely a North American phenomenon). Acts of sabotage by one commercial entity against another are rare but not unheard of and I've investigated more than one.
- **Acts by a foreign power** – At the end of the Cold War, a downsizing of the traditional intelligence agencies was inevitable as many field operatives suffered from a 'reduction in force' (RIF). However, many ex-KGB officers (for example) are now in engaged in commercial espionage, a great deal of it state sanctioned. Industrial intelligence gathering against the US and Western European nations is a major remit of the Russian intelligence-gathering apparatus, in particular the Foreign Intelligence Service (SVR, the successor to the KGB) and, to a lesser extent, the military intelligence organization (GRU). Favorite targets include government contractors.
- **Terrorism** – In the 1980s and 1990s, British government departments and their counterparts in the commercial sector were targeted by various groups with no small degree of success. As one group is neutralized, new threats emerge to take their place. MI5 currently monitors thousands of potential terrorists and hardly a week seems to go by without new suspects being arrested.

In conclusion, the complexity and range of the threat is far more involved than it initially appears to be. The climate we live in makes security everybody's problem and it's critical that every organization, large or small, understands the risks and is prepared for them.

Engaging a Penetration Testing Team

This chapter covers the basics of physical penetration and its goals. You may be reading this with the intention of engaging a company to carry out a physical test. Before you read any further you should consider the costs, potential benefits and limitations associated with such an exercise. Is this really something you need? Is it really something that your organization will benefit from? Other questions you should ask yourself are these:

- Do you currently have an all-encompassing security policy?
- Are you auditing against that policy?

- What do you wish you learn from the exercise?
- Are there specific areas you lack confidence in and want tested?
- Should the test be black box or crystal box?
- How do you expect your organization to fare?
- Are you engaging a test to justify additional security budget?

If you don't have a security policy, then implementing one should be your priority. If you don't expect to perform very well in the test, consider why this is and implement additional security controls in these areas. If you don't feel you have sufficient budget and are looking to boost it with demonstrable security weaknesses then don't worry, you're not alone. In fact, this is the number one reason that companies engage in any form of penetration test for the first time.

Summary

This chapter has covered the basics of what you need to know if you want to get to grips with the somewhat involved field of physical penetration testing. There's a lot more to cover beyond the essentials introduced here.

There's much more to security than just the technical aspects and there's much more to technical security than just buffer overflows. You've looked a little at what penetration testers do when faced with physical assignments as well the history of the industry and how it grew largely out of its military infancy into the commercial sector as the need arose.

Most importantly, I have covered the basic terminology, which is critical to understanding later material. Getting used to the terminology also gets you into right mindset.

I've also introduced a little of why you would want conduct this form of testing and the threats that different organizations face. If you're reading this book from the perspective of a security manager or CIO you should be a little clearer on what's involved in hiring a testing team.