# Chapter 8

# Exploiting Physical and Social Vulnerabilities

# Outlines

- Physical Facility Penetration Testing
- Entering Facilities
- Piggybacking and Tailgating
- Bypassing Locks and Entry Control Systems
- Bypassing Perimeter Defenses and Barriers
- Information Gathering
- Social Engineering
- In-Person Social Engineering
- Elicitation
- Interrogation and Interviews
- Impersonation
- Quid Pro Quo
- Shoulder Surfing
- USB Key Drops
- Bribery
- Phishing Attacks
- Website-Based Attacks
- Watering Holes
- Cloned Websites
- Using Social Engineering Tools

## Physical Facility Penetration Testing

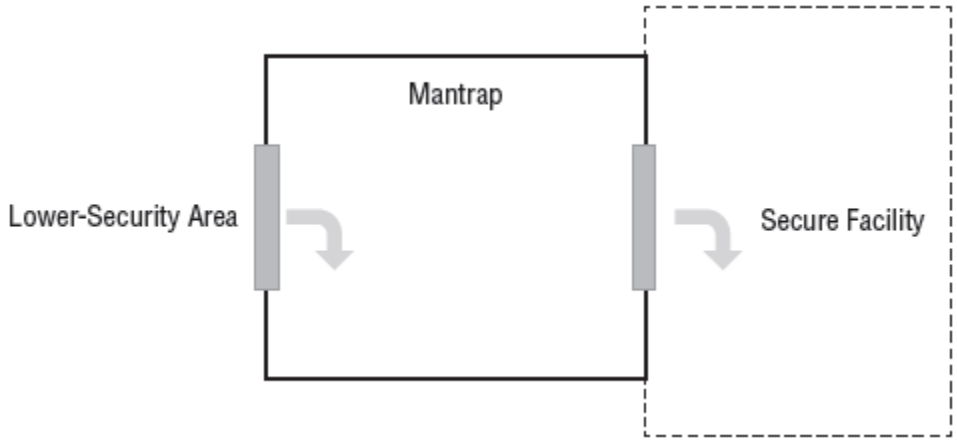
Physical access to systems, networks, and facilities can provide opportunities that remote network attacks can't. In most cases, direct physical access is one of the best ways to gain higher-level access, making physical penetration tests a powerful tool in a pen-tester's arsenal. Physical penetration tests are also a very useful way to test the effectiveness of physical security controls like entry access systems, sensors and cameras, security procedures, and guards, as well as security training for staff. Much like network-based assessments, physical penetration tests require information gathering, analysis, exploitation, and reporting.

## Entering Facilities

Gaining access to a facility is one of the first steps once you begin your onsite assessment. Figuring out how to get into public areas is often relatively easy, but secured areas usually require more work. You may have to pick locks or find another way to bypass them, or you may have to use social engineering techniques to persuade staff members to let you in.

# Piggybacking and Tailgating

One of the easiest ways into a facility is to accompany a legitimate employee. If you look like you belong in the facility, and the organization is one in which not all employees know each other, piggybacking is a good option. Piggybacking attacks rely on following employees in through secured doors or other entrances. Higher-security organization may use mantraps to prevent piggybacking and tailgating. A properly implemented mantrap




While piggybacking can be a useful solution, other related techniques include dressing as a delivery driver and bringing a box or other delivery in or finding another likely reason to be admitted by employees. Even if they won't let you follow them in because of security concerns, there is almost always a reason that will persuade them to open the door for you!

## Bypassing Locks and Entry Control Systems

**Entry control is often managed through locks, making picking locks a useful part of a penetration tester's toolkit. Many penetration testers carry a lockpick set that can allow them to bypass many locks that they encounter, including those on doors, desks, filing cabinets, and other types of secure storage.**

- **Deviant Ollam's site: http://deviating.net/lockpicking/**
- **TheLockWiki : http://www.lockwiki.com/index.php/Locksprt**
- **The Open Organization Of Lockpickers (TOOOL) website: https://toool.us**

**Bypassing locks that don't use keys can also be useful—so you also need to pay attention to RFID and magnetic stripe access card systems and cloning tools, as well as any other entry access mechanisms in use in the organization. Push-button locks, electronic keypads, and other mechanisms may be used, and gaining access can be as simple as watching for a legitimate user to punch in their code in plain sight! Lock bypass techniques also involve tools like "shove keys," which are thin metal shims that can be hooked over latches and locks to allow a penetration tester to disengage the lock. Specialized shims and other tools—including simply putting a piece of tape over the latch plate of an exit door so you can reenter later—are all methods used to bypass locks without picking them.**

## Bypassing Perimeter Defenses and Barriers

Fences and other barriers are intended as both physical barriers and deterrents to unauthorized access. Fences come in many styles, from low fences intended to limit traffic or prevent casual access to higher-security fences topped with barbed wire or razor wire to discourage climbers. Very high-security locations may even reinforce their fences with aircraft cable to prevent vehicles from crashing through them and may extend their fences below ground level to discourage digging under them. As you might expect, organizations that use higher-security fence designs are also likely to have guard posts, including gate guards, and may even have security patrols.

### Common Controls:

- Alarms, which may need to be bypassed or disabled
- Lighting, including motion-activated lighting
- Motion sensors that may activate alarm systems
- Video surveillance and camera systems that may record your activities

## Information Gathering

Gathering information while in a facility can provide useful information for both physical and network-based penetration testing. Many penetration testers will record their entire physical penetration test attempt using a concealed camera and will also record any reconnaissance activities. This allows them to review the footage to find security cameras, employee badge numbers, and many other pieces of information they might miss if they relied only on memory and notes. Penetration testers also often engage in dumpster diving, or retrieving information from the organization's trash.

# Social Engineering

Social engineering targets people instead of computers and relies on individuals or groups breaking security procedures, policies, and rules. In the context of the PenTest+ exam, a social engineer finds and exploits human weaknesses and behaviors to accomplish the goals of a penetration test. Social engineering can be done in person, over the phone, via text messaging or email, or in any other medium where the social engineer can engage and target the people who work for or with a target organization.

- **Trust** is the foundation of many social engineering attacks. Creating a perception of trust can be done in many ways. Most individuals unconsciously want to trust others, providing a useful target for social engineers!
- **Reciprocation** relies on the target feeling indebted, or that they need to return a favor.
- **Authority** focuses on making the target believe that you have the power or right to ask them to perform actions or provide information.
- **Urgency** is the sense that the action needs to be performed, often because of one of the other reasons listed here
- **Fear** that something will go wrong or that they will be punished if they do not respond or help is a common target.
- **Likeness** or **similarity** between the social engineer and the target is a means of building trust, as the target is set up to sympathize with the pen-tester due to their similarity.
- **Social proof** relies on persuading the target that other people have behaved similarly and, thus, that they should or could as well.
- **Scarcity** is related to fear-based approaches but focuses on there being fewer rewards or opportunities, requiring faster action and thus creating a sense of urgency.
- **Helpful nature** is the straightforward truth about most decent people. When given an innocent opportunity to be appreciated, a target will be helpful to the pen-tester.

## In-Person Social Engineering

In-person social engineering requires a strong understanding of individuals and how they respond, and it leverages the social engineer's skills to elicit desired responses. There are many in-person social engineering techniques, including those documented in the Social Engineering Framework: https://www.social-engineer.org/framework/general-discussion/.

## Elicitation

Gathering information is a core element of any social engineering exercise, and elicitation, or getting information without directly asking for it, is a very important tool. Asking an individual for information directly can often make them suspicious, but asking other questions or talking about unrelated areas that may lead them to reveal the information you need can be very effective. Common techniques include using open-ended or leading questions and then narrowing them down as topics become closer to the desired information.

## Interrogation and Interviews

Interrogation and interview tactics can be used as part of a social engineering process. Interrogation techniques focus on the social engineer directing the conversation and asking most, if not all, of the questions. This is less subtle and less comfortable for the target, and it means that interrogation is less frequently used unless the target has a reason to allow being interrogated. Interview tactics are similar but place the subject more at ease. In both cases, body language is an important clue to the target's feelings and responses.

## Impersonation

Many social engineering techniques involve some form of impersonation. Impersonation involves disguising yourself as another person to gain access to facilities or resources. This may be as simple as claiming to be a staff member or as complex as wearing a uniform and presenting a false or cloned company ID. Impersonating a technical support worker, maintenance employee, delivery person, or administrative assistant is also common. Impersonation frequently involves pretexting, a technique where the social engineer claims to need information about the person they are talking to, thus gathering information about the individual so that they can better impersonate them.

## Quid Pro Quo

**Quid pro quo attacks** rely on the social engineer offering something of value to the target in order for the target to feel safe and indebted to them. This builds perceived trust, luring the target into feeling safe in returning the favor.

## Shoulder Surfing

Simply watching over a target's shoulder can provide valuable information like passwords or access codes. This is known as shoulder surfing, and high-resolution cameras with zoom lenses can make it possible from long distances.

## USB Key Drops

**Physical honeypots like USB keys or other media can be used when other means of accessing an organization aren't possible.** To perform this type of attack, the penetration tester preloads a thumb drive with attack tools aimed at common operating systems or software found in the target company. They then drop one or more of these drives in locations where they are likely to be found, sometimes with a label that indicates that the drive has interesting or important data on it.

## Bribery

Bribing employees at the target organization to allow you to access systems or facilities will not be in scope for many penetration tests, but penetration testers should be aware that it may be a valid technique under some circumstances. Bribery is a sensitive topic and should be carefully addressed via scoping agreements and the rules of engagement for a penetration test.

## Phishing Attacks

Phishing attacks target sensitive information like passwords, usernames, or credit card information. While most phishing is done via email, there are many related attacks that can be categorized as types of phishing:

- Vishing , or voice phishing, is social engineering over the phone system.
- SMS phishing, or smishing, is phishing via SMS messages.
- Whaling targets high-profile or important members of an organization like the CEO or senior vice presidents.
- Spear phishing is aimed at specific individuals rather than a broader group.

## Website-Based Attacks

While many social engineering attacks are done via phishing or in-person techniques, a web-based social engineering attack can also be a useful tool. Two of the most commonly used website-based attacks are watering holes and the use of cloned websites for phishing.

## Watering Holes

Once you have learned the behaviors of staff at a target organization, you may identify a commonly visited site. Attacks that focus on compromising a site like this and modifying its code to include malware is known as a watering hole attack. Watering hole attacks may focus on the code of the site itself or code that the site includes by default, such as ad code or the plug-ins. This often combines social engineering with traditional application, server, or service attacks to complete the watering hole attack successfully.

## Cloned Websites

Many phishing attacks rely on cloned websites. Such a site appears to be a real website but instead captures data that is entered. Some then pass that data along to the real website, but others simply redirect you elsewhere after capturing the data. Cloning many websites is as easy as saving the code, and tools like the Social Engineering Toolkit provide website attack vector tools that can clone a website for phishing or malicious code injection.

## Using Social Engineering Tools

Social engineering techniques are powerful, but combining them with technical tools that allow for the use of pre-built attack vectors and automation can give a penetration tester a major advantage. Fortunately, attack tools designed specifically to support penetration testing exist. Two of the most common tools are the Social Engineering Toolkit, or SET, and the Browser Exploitation Framework, or BeEF.

## Questions

**1. Cynthia wants to use a phishing attack to acquire credentials belonging to the senior leadership of her target. What type of phishing attack should she use?**

**A. Smishing**

**B. VIPhishing**

**C. Whaling**

**D. Spear phishing**

**2. Mike wants to enter an organization's high-security data center. Which of the following techniques is most likely to stop his tailgating attempt?**

**A. Security cameras**

**B. A mantrap**

**C. An egress sensor**

**D. An RFID badge reader**

**3. Which of the following technologies is most resistant to badge cloning attacks if implemented properly?**

**A. Low frequency RFID**

**B. Magstripes**

**C. Medium frequency RFID**

**D. Smart cards**

**Use the following scenario for questions 4, 5, and 6. Jen has been contracted to perform a penetration test against Flamingo, Inc. As part of her penetration test, she has been asked to conduct a phishing campaign and to use the results of that campaign to gain access to Flamingo systems and networks. The scope of the penetration test does not include a physical penetration test, so Jen must work entirely remotely.**

**4. Jen wants to send a phishing message to employees at the company. She wants to learn the user IDs of various targets in the company and decides to call them using a spoofed VoIP phone number similar to those used inside the company. Once she reaches her targets, she pretends to be an administrative assistant working with one of Flamingo's senior executives and asks her targets for their email account information. What type of social engineering is this?**

**A. Impersonation**

**B. Interrogation**

**C. Shoulder surfing**

**D. Administrivia**

**5. Jen wants to deploy a malicious website as part of her penetration testing attempt so that she can exploit browsers belonging to employees. What framework is best suited to this?**

**A. Metasploit**

**B. BeEF**

**C. SET**

**D. OWASP**

**6. After attempting to lure employees at Flamingo, Inc., to fall for a phishing campaign, Jen finds that she hasn't acquired any useful credentials. She decides to try a USB key drop. Which of the following Social Engineering Toolkit modules should she select to help her succeed?**

**A. The website attack vectors module**

**B. The Infectious Media Generator**

**C. The Mass Mailer Module**

**D. The Teensy USB HID attack module**

**7. Chris sends a phishing email specifically to Susan, the CEO at his target company. What type of phishing attack is he conducting?**

**A. CEO baiting**

**B. Spear phishing**

**C. Phish hooking**

**D. Hook SETting**

**8. While Frank is performing a physical penetration test, he notices that the exit doors to the data center open automatically as an employee approaches them with a cart. What should he record in his notes?**

**A. The presence of an egress sensor**

**B. The presence of a mantrap**

**C. A potential unlocked door**

**D. Nothing because this is not a vulnerability**

**9. Emily wants to gather information about an organization, but does not want to enter the building. What physical data gathering technique can she use to potentially gather business documents without entering the building?**

**A. Piggybacking**

**B. File surfing**

**C. USB drops**

**D. Dumpster diving**

**10. Cameron is preparing to travel to another state to perform a physical penetration test. What penetration testing gear should he review the legality of before leaving for that state?**

**A. Metasploit**

**B. Lockpicks**

**C. Encryption tools**

**D. SET**

**11. Which social engineering motivation technique relies on persuading the target that other people have behaved similarly and thus that they could too?**

**A. Likeness**

**B. Fear**

**C. Social proof**

**D. Reciprocation**

**12. What is the default read-only community string for many SNMP devices?**

**A. secret**

**B. readonly**

**C. private**

**D. public**

**13. Allan wants to gain access to a target company's premises but discovers that his original idea of jumping the fence probably isn't practical. Which factor is least likely to prevent him from trying to jump the fence?**

**A. Barbed wire**

**B. A gate**

**C. Fence height**

**D. Security guards**

**14. Charles sends a phishing email to a target organization and includes the line "Only five respondents will receive a cash prize." Which social engineering motivation strategy is he using?**

**A. Scarcity**

**B. Social proof**

**C. Fear**

**D. Authority**

**15. What occurs during a quid pro quo social engineering attempt?**

**A. The target is offered money.**

**B. The target is asked for money.**

**C. The target is made to feel indebted.**

**D. The penetration tester is made to feel indebted.**

16. Andrew knows that the employees at his target company frequently visit a football discussion site popular in the local area. As part of his penetration testing, he successfully places malware on the site and takes over multiple PCs belonging to employees. What type of attack has he used?

A. A PWNie attack

B. A watercooler attack

C. A clone attack

D. A watering hole attack

17. Steve inadvertently sets off an alarm and is discovered by a security guard during an on-site penetration test. What should his first response be?

A. Call the police

B. Attempt to escape

C. Provide his pretext

D. Call his organizational contact

18. A USB key drop is an example of what type of technique?

A. Physical honeypot

B. A humanitarian exploit

C. Reverse dumpster diving

D. A hybrid attack

**19. Susan calls staff at the company she has been contracted to conduct a phishing campaign against, focusing on individuals in the finance department. Over a few days, she persuades an employee to send a wire transfer to an account she has set up after telling the employee that she has let their boss know how talented they are. What motivation technique has she used?**

**A. Urgency**

**B. Reciprocation**

**C. Authority**

**D. Fear**

**20. Alexa carefully pays attention to an employee as they type in their entry code to her target organization's high security area and writes down the code that she observes. What type of attack has she conducted?**

**A. A Setec Astronomy attack**

**B. Code surveillance**

**C. Shoulder surfing**

**D. Keypad capture**