**CHAPTER 4 SOCIAL ENGINEERING, PHYSICAL, AND PASSWORD ATTACKS**

Social engineering techniques focus on the human side of information security. Using social engineering techniques, security professionals and attackers can accomplish a variety of tasks ranging from acquiring information to gaining access to buildings, systems, and networks.

This chapter explores social engineering techniques and related practices, from dumpster diving to shoulder surfing and whaling. We discuss the principles that underlie social engineering attacks, as well as how modern influence campaigns use social engineering concepts and social media to sway opinions and reactions.

Social engineering and phishing attacks often precede password attacks, and later in this chapter you will review password attack methods like brute-force attacks, rainbow tables, and dictionary attacks. Physical attacks that penetration testers and attackers can use in person complete your exploration of these attack methodologies.

**SOCIAL ENGINEERING**

Social engineering is the practice of manipulating people through a variety of strategies to accomplish desired actions. Social engineers work to influence their targets to take actions that they might not otherwise have taken.

A number of key principles are leveraged to successfully social engineer an individual, and though the list of principles and their names vary depending on the source you read, the Security+ exam focuses on seven:

* Authority, which relies on the fact that most people will obey someone who appears to be in charge or knowledgeable, regardless of whether or not they actually are. A social engineer using the principle of authority may claim to be a manager, a government official, or some other person who would have authority in the situation they are operating in.
* Intimidation relies on scaring or bullying an individual into taking a desired action. The individual who is targeted will feel threatened and respond by doing what the social engineer wants them to do.
* Consensus-based social engineering uses the fact that people tend to want to do what others are doing to persuade them to take an action. A consensus-based social engineering attack might point out that everyone else in a department had already clicked on a link, or might provide fake testimonials about a product making it look safe. Consensus is called “social proof” in some categorization schemes.
* Scarcity is used for social engineering in scenarios that make something look more desirable because it may be the last one available.
* Familiarity-based attacks rely on you liking the individual or even the organization the individual is claiming to represent.
* Trust, much like familiarity, relies on a connection with the individual they are targeting. Unlike with familiarity, which relies on targets thinking that something is normal and thus familiar, social engineers who use this technique work to build a connection with their targets so that they will take the actions that they want them to take.
* Urgency relies on creating a feeling that the action must be taken quickly due to some reason or reasons.

You may have noticed that each of these social engineering principles works because it causes the target to react to a situation, and that many make the target nervous or worried about a result or scenario. Social engineering relies on human reactions, and we are most vulnerable when we are responding instead of thinking clearly.

Many, if not most, social engineering efforts in the real world combine multiple principles into a single attack. If a penetration tester calls claiming to be a senior leader's assistant in another part of your company (thus leading authority and possibly familiarity responses) and then insists that that senior leader has an urgent need (urgency) and informs their target that they could lose their job if they don't do something immediately (intimidation), they are more likely to be successful in many cases than if they only used one principle. A key part of social engineering is understanding the target, how humans react, and how stress reactions can be leveraged to meet a goal.

**SOCIAL ENGINEERING TECHNIQUES**

Social engineering involves more than the principles you just read. There are both technical and nontechnical attacks that leverage those principles to get results that are desired by both attackers and penetration testers. As a security professional, you need to be aware of these techniques, what they involve, and what makes each of them different from the others.

**PHISHING**

Phishing is a broad term used to describe the fraudulent acquisition of information, often focused on credentials like usernames and passwords, as well as sensitive personal information like credit card numbers and related data. Phishing is most often done via email, but a wide range of phishing techniques exist, including things like smishing, which is phishing via SMS (text) messages, and vishing, or phishing via telephone.

Specific terms are also used for specific targeting of phishing attempts. Spear phishing targets specific individuals or groups in an organization in an attempt to gather desired information or access. Whaling, much like spear phishing, targets specific people, but whaling is aimed at senior employees like CEOs and CFOs, “big fish” in the company, thus the term whaling.

Like most social engineering techniques, one of the most common defenses against phishing of all types is awareness. Teaching staff members about phishing and how to recognize and respond to phishing attacks, and even staging periodic exercises, are all common means of decreasing the risk of successful phishing attacks. Technical means also exist, including filtering that helps prevent phishing using reputation tools, keyword and text pattern matching, and other technical methods of detecting likely phishing emails, calls, or texts.

**CREDENTIAL HARVESTING**

Credential harvesting is the process of gathering credentials like usernames and passwords. Credential harvesting is often performed via phishing attacks but may also be accomplished through system compromise resulting in the acquisition of user databases and passwords, use of login or remote access tools that set up to steal credentials, or any other technique that will gather credentials for attackers.

Once credentials are harvested, attackers will typically leverage them for further attacks, with financial attacks a top target. Although credential harvesting can be difficult to completely stop, multifactor authentication (MFA) remains a strong control that can help limit the impact of successful credential harvesting attacks. User awareness, technical tools that can stop harvesting attacks like phishing emails or related techniques, and strong monitoring and response processes can all help with credential harvesting and abuse of harvested credentials.

example, how are spear phishing and whaling different?

**WEBSITE ATTACKS**

Attacks against websites are also used by social engineers, and pharming is one example. Pharming attacks redirect traffic away from legitimate websites to malicious versions. Pharming typically requires a successful technical attack that can change DNS entries on a local PC or on a trusted local DNS server, allowing the traffic to be redirected.

Typo squatters use misspelled and slightly off but similar to the legitimate site URLs to conduct typosquatting attacks. Typo squatters rely on the fact that people will mistype URLs and end up on their sites, thus driving ad traffic or even sometimes using the typo-based website to drive sales of similar but not legitimate products.

Unlike pharming, watering hole attacks don't redirect users; instead, they use websites that targets frequent to attack them. These frequently visited sites act like a watering hole for animals and allow the attackers to stage an attack, knowing that the victims will visit the site. Once they know what site their targets will use, attackers can focus on compromising it, either by targeting the site or deploying malware through other means such as an advertising network.

**SPAM**

Spam, sometimes called unsolicited or junk email, may not immediately seem like a social engineering technique, but spam often employs social engineering techniques to attempt to get recipients to open the message or to click on links inside of it. In fact, spam relies on one underlying truth that many social engineers will take advantage of: if you send enough tempting messages, you're likely to have someone fall for it!

The Security+ exam outline also includes Spam over Instant Messaging (SPIM). While the term appear on the exam outline, SPIM never really became a widely used term in the security industry. You should still make sure you know it for the exam, and that it specifically describes instant messaging spam.

**IN-PERSON TECHNIQUES**

Although many of the techniques we have discussed so far rely on technology to accomplish them, in-person social engineering and penetration testing techniques are also important to know. The Security+ exam outline includes a number of in-person techniques such as dumpster diving, shoulder surfing, and tailgating.

Although it isn't really a social engineering technique, dumpster diving is a very effective information gathering technique. It is exactly what it sounds like: retrieving potentially sensitive information from a dumpster. Dumpster diving can provide treasure troves of information about an organization, including documentation and notes. Organizations that want to avoid this will secure their dumpsters, use secure disposal services for documents, and will otherwise seek to ensure that their trash really is trash without anything useful in it.

Shoulder surfing is the process of looking over a person's shoulder to capture information like passwords or other data. Although shoulder surfing typically implies actually looking over a person's shoulder, other similar attacks such as looking into a mirror behind a person entering their credentials would also be considered shoulder surfing. Preventing shoulder surfing requires awareness on the part of potential targets, although tools like polarized security lenses over mobile devices like laptops can help prevent shoulder surfing in public spaces.

Tailgating is a physical entry attack that requires simply following someone who has authorized access to an area so that as they open secured doors you can pass through as well. Much like shoulder surfing, tailgating is best prevented by individual awareness. If someone attempts to follow you through a secure door, you should make them present their own credentials instead of letting them in or report the intrusion immediately!

Eliciting information, often called elicitation, is a technique used to gather information without targets realizing they are providing it. Techniques like flattery, false ignorance, or even acting as a counselor or sounding board are all common elements of an elicitation effort. Talking a target through things, making incorrect statements so that they correct the person eliciting details with the information they need, and other techniques are all part of the elicitation process. Ideally, a social engineering target who has experienced an elicitation attack will never realize they have provided more information than they intended to, or will only realize it well after the fact.

Prepending can mean one of three things:

* Adding an expression or phrase, such as adding “SAFE” to a set of email headers to attempt to fool a user into thinking it has passed an antispam tool
* Adding information as part of another attack to manipulate the outcome
* Suggesting topics via a social engineering conversation to lead a target toward related information the social engineer is looking for

**IDENTITY FRAUD AND IMPERSONATION**

Pretending to be someone else is a key tool in a social engineer's toolkit, and like all of the other social engineering techniques we have discussed, it can be used for malicious purposes. Each of these techniques combines the willingness of the target or targets to believe the impersonator with the principles of social engineering to create a scenario where the social engineer will get the access, data, or other results they desire.

Pretexting is the process of using a made-up scenario to justify why you are approaching an individual. Pretexting is often used as part of impersonation efforts to make the impersonator more believable. An aware target can ask questions or require verification that can help defeat pretexting and impersonation attacks. In many cases, simply making a verification call can defeat such attempts.

Identity fraud, or identity theft, is the use of someone else's identity. Although identity fraud is typically used for financial gain by malicious actors, identity fraud may be used as part of penetration tests or other security efforts as well. In fact, in some cases impersonation, where you act as if you are someone else, can be a limited form of identity fraud. In other cases, impersonation is less specific, and the social engineer or attacker who uses it may simply pretend to be a delivery driver or an employee of a service provider rather than claiming a specific identity.

In addition to these more direct individual interactions, hoaxes are a common occurrence. Hoaxes, which are intentional falsehoods, come in a variety of forms ranging from virus hoaxes to fake news. Social media plays a large role in many modern hoaxes, and attackers and social engineers may leverage current hoaxes to assist in their social engineering attempts.

A final type of fraud is the use of invoice scams, which involve sending fake invoices to organizations in the hopes of receiving payment. Invoice scams can be either physical or electronic, and they rely on the recipient not checking to see if the invoice is legitimate.

**RECONNAISSANCE AND IMPERSONATION**

Social engineering is a great way to gather information and thus is often used as part of reconnaissance efforts. Social engineering can be used during phone calls, email, and other means of contact to elicit more information about a target than is publicly available. At the same time, on-site and in-person reconnaissance efforts use social engineering techniques to gain access, gather information, and bypass security systems and processes.

**INFLUENCE CAMPAIGNS**

As cyberwarfare and traditional warfare have continued to cross over in deeper and more meaningful ways, online influence campaigns, which have traditionally focused on social media, email, and other online-centric mediums, have become part of what has come to be called hybrid warfare. Although the formal definition of hybrid warfare is evolving, it is generally accepted to include competition short of conflict, which may include active measures like cyberwarfare as well as propaganda and information warfare.

Influence campaigns themselves are not the exclusive domain of cyberwarfare, however. Individuals and organizations conduct influence campaigns to turn public opinion in directions of their choosing. Even advertising campaigns can be considered a form of influence campaign, but in general, most influence campaigns are associated with disinformation campaigns. For the Security+ exam, you should be aware of the tightly coupled roles of influence campaigns and social media as part of hybrid warfare efforts by nation-state actors of all types.

**PASSWORD ATTACKS**

Although social engineering is often used to acquire passwords or access, there are other ways to attack passwords as well. Everything from trying password after password in a brute-force attack to technical attacks that leverage precomputed password hashes in lookup systems to check acquired password hashes against a known database, can help attackers and penetration testers attack passwords.

The Security+ exam focuses on a few critical password-related attacks:

* Brute-force attacks, which iterate through passwords until they find one that works. Actual brute-force methods can be more complex than just using a list of passwords and often involve word lists that use common passwords, words specifically picked as likely to be used by the target, and modification rules to help account for complexity rules. Regardless of how elegant or well thought out their input is, brute force in the end is simply a process that involves trying different variations until it succeeds.
* Password spraying attacks are a form of brute-force attack that attempts to use a single password or small set of passwords against many accounts. This approach can be particularly effective if you know that a target uses a specific default password or a set of passwords. For example, if you were going to attack a sports team's fan website, common chants for the fans, names of well-known players, and other common terms related to the team might be good candidates for a password spraying attack.
* Dictionary attacks are yet another form of brute-force attack that uses a list of words for their attempts. Commonly available brute-force dictionaries exist, and tools like John the Ripper, a popular open source password cracking tool, have word lists (dictionaries) built in. Many penetration testers build their own custom dictionaries as part of their intelligence gathering and reconnaissance processes.

Regardless of the password attack mechanism, an important differentiator between attack methods is whether they occur online, and thus against a live system that may have defenses in place, or if they are offline against a compromised or captured password store. If you can capture hashed passwords from a password store, tools like rainbow tables can be very useful. Rainbow tables are an easily searchable database of precomputed hashes using the same hashing methodology as the captured password file. Thus, if you captured a set of passwords that were hashed using MD5, you could compute or even purchase a full set of passwords for most reasonable password lengths, and then simply look up the hashes of those passwords in the table.

If you have captured a password file, you can also use a password cracker against it. Password crackers like John the Ripper, shown in Figure 4.1, attempt to crack passwords by trying brute-force and dictionary attacks against a variety of common password storage formats.

Une image contenant texte

Description générée automatiquement

FIGURE 4.1 John the Ripper

TP: Learning how to use tools like John the Ripper can help you understand both password cracking and how passwords are stored. You can find a variety of exercises at openwall.info/wiki/john/tutorials that will get you started.

Password cracking tools like John the Ripper can also be used as password assessment tools. Some organizations continue to periodically test for weak and easily cracked passwords by using a password cracker on their password stores. In many cases, use of MFA paired with password complexity requirements have largely replaced this assessment process, and that trend is likely to continue.

Of course, not every system is well maintained, and a penetration tester or attacker's favorite opportunity is finding plain-text or unencrypted passwords to acquire. Without some form of protection, passwords that are just maintained in a list can be easily acquired and reused by even the most casual of attackers. As noted earlier, using a strong password hashing mechanism, as well as techniques like using a salt and a pepper (additional data added to passwords before they are hashed, making it harder to use tools like rainbow tables) can help protect passwords. In fact, best practices for password storage don't rely on encryption; they rely on passwords never being stored and instead using a well-constructed password hash to verify passwords at login.

TP : If you want to learn more about secure password storage, OWASP maintains a great cheat sheet at cheatsheetseries.owasp.org/cheatsheets/Password\_Storage\_Cheat\_Sheet.html.

**PHYSICAL ATTACKS**

Social engineering and on-site penetration testing often go hand in hand, and thus the physical side of social engineering has its own set of tools and techniques. The Security+ exam outline covers a few of the most common examples, and you will need to be aware of each of these to be prepared for the exam.

Malicious flash drive attacks largely fall into two categories. Penetration testers (and potentially attackers) may drop drives in locations where they are likely to be picked up and plugged in by unwitting victims at their target organization. An additional layer of social engineering is sometimes accomplished by labeling the drives with compelling text that will make them more likely to be plugged in: performance reviews, financial planning, or other key words that will tempt victims.

Malicious flash drives and other devices are also sometimes effectively a Trojan, as when devices have shipped or been delivered with malware included either from the factory or through modifications made in the supply chain. This was particularly prevalent with digital picture frames in the past, but any USB-connected device that can store files is a potential carrier for this type of attack, even if it isn't a USB thumb drive.

Malicious USB cables also exist, although they're less common since they require dedicated engineering to build, rather than simply buying commodity flash drives. The advantage of a malicious USB cable is that it can be effectively invisible when it replaces an existing cable and will not be noticed in the same way that a flash drive might be. Malicious cables are often configured to show up as a human interface device (e.g., a keyboard) and may be able to interface with the computer to send keystrokes or capture data in addition to deploying malware.

TP : Forensic tools like USB Historian (4discovery.com/our-tools/usb-historian) can help identify devices that were plugged into Windows systems, allowing incident responders to learn more about what devices might have been malicious and to look for other systems they may have been connected to.

Card cloning attacks focus on capturing information from cards like RFID and magnetic stripe cards often used for entry access. Attackers may also conduct skimming attacks that use hidden or fake readers or social engineering and hand-held readers to capture (skim) cards, and then employ cloning tools to use credit cards and entry access cards for their own purposes. Card cloning can be difficult to detect if the cards do not have additional built-in protection such as cryptographic certificates and smart chips that make them hard to clone. Magnetic stripe and RFID-based cards that can be easily cloned can often be detected only by visual inspection to verify that they are not the original card.

A final option for physical attacks is an attack on the supply chain for the organization. Supply chain attacks attempt to compromise devices, systems, or software before it even reaches the organization. In the United States, the government is concerned enough about this issue that it operates the Trusted Foundry under the auspices of the U.S. Department of Defense. The Trusted Foundry program ensures that the supply chain for classified and unclassified integrated circuits, devices, and other critical elements are secure and that manufacturers stay in business and are protected appropriately to ensure that trusted devices remain trusted.

For individual organizations, supply chain security is much harder, but buying from trusted vendors rather than secondary market providers, as well as ensuring that devices are not modified by third parties by using physical security measures like tamper-evident holographic seal stickers, can help ensure that supply chain attacks are less likely to occur.

Attacks in the Cloud versus Attacks on Premises

Moving to the cloud changes which attacks you are likely to worry about in a number of cases, as well as which controls you can deploy and manage. For most organizations, outsourcing to a cloud service provider means that you are likely to be operating in what may potentially be a more secure datacenter, and one in which it would be far harder to figure out which systems your operations are running. At the same time, you will no longer have the ability to audit access to the facility or to check on what occurred to a specific physical machine.

As you consider attack and defense scenarios, you will need to carefully consider how the cloud versus on-premises security concerns impact your organization. The Security+ exam outline specifically calls this thought process out, so as you read through this book, think about which technologies, practices, and capabilities you would need or not need in each environment.

Summary

Social engineering techniques focus on human reactions and psychology to gather information and to perform attacks against individuals and organizations. The broad range of social engineering techniques rely on common principles that describe ways to influence people based on their reaction to pressures or stress.

Security professionals need to be aware of how social engineering is leveraged in attacks like phishing, impersonation, and reconnaissance efforts. Each technique has its own distinctive set of social engineering techniques and impacts that help make it unique.

Physical attacks against organizations also rely on social engineering concepts to help them succeed. Use of malicious USB devices like cables and flash drives take advantage of human behavior to lure users into plugging them in, and attacks against access cards may use skimmers or other techniques to allow cloning of the access cards used by an organization.

Password attacks focus on acquisition of passwords in an encrypted, hashed, or plain-text form, or on guessing passwords in order to gain access to systems or devices.

All of these attacks need to be assessed and considered in the operating environment of your organization. As organizations move from local physical infrastructure to cloud services, the threat and attack models that you must consider also need to change.