1 A Look into the New World of Professional Social Engineering

1. social engineering from a malicious perspective - SMiShing, Vishing, Phishing, Impersonation
2. The SE Pyramid: OSINT, Pretext Development, Attack Plan, Attack Launch, Reporting
3. And that is exactly the goal of the malicious social engineer: to get the target to take an action that is not in their best interest without thinking through the potential dangers involved.

2 Do You See What I See?

Remember that failure is an event, not a person

1. Corporation: How does the corporation use the Internet? How does the corporation use social media? Does the corporation have policies in place for what its people can put on the Internet? How many vendors does the corporation have? What vendors does the corporation use? How does the corporation accept payments? How does the corporation issue payments? Does the corporation have call centers? Where are headquarters, call centers, or other branches located? Does the corporation allow BYOD (bring your own device)? Is the corporation in one location or many locations? Is there an org chart available?
2. Individual: What social media accounts does the person use? What hobbies does the person have? Where does the person vacation? What are the person's favorite restaurants? What is the family history (sicknesses, businesses, and so on) of the person? What is the person's level of education? What did the person study? What is the person's job role, including whether people work from home, for themselves, and who they report to? Are there any other sites that mention the person (maybe they give speeches, post to forums, or are part of a club)? Does the person own a house? If yes, what are the property taxes, liens, and so on? What are the names of the person's family members (as well as any of the previously mentioned info on those people)?
3. Fortunately, one of the oldest forms of OSINT proved to be in the researcher's favor: listening.
4. different sections like Personal, Business, Family, Social Media
5. The important thing is that you take seriously how you store, manage, back up, transmit, and secure any data you collect on your clients.

Nontechnical OSINT - Observational Skills

1. OSINT arsenal of observational skills: Clothing, Entries and exits, Requirements for entry, Perimeter security, Security staff, Lobby Setup
2. We did not observe the little detail in this story, and that lack of observation cost us. The lesson of this scenario is that you need to observe everything you can. Think like the person you are social engineering. Try to understand what they would expect to see, and deliver that. Otherwise, little details can come back to bite you.

What Can You Do to Teach Yourself These Skills?

1. Gender of X number of people
2. What they were wearing

3. What activities the people were engaged in when I first sighted them
4. Perceived communication profile
5. Body-language tells
6. My suggestion is to look for your own weaknesses, and then start small and build up.
7. Failure can teach us way more than success if we let it— which is why I need to talk about expectations.

Technical Open Source Intelligence

Social Media

1. LinkedIn: Your job history Where you got your education Where you went to high school Clubs and academic achievements you're involved in People who endorse your skills
2. Facebook: Your favorite music Your favorite movies Clubs you belong to Your friends Your family Vacations you've taken Your favorite foods Places you've lived
3. Twitter: What you are doing right now Your eating habits Your geolocation Your emotional state
4. Evaluating a person based on social media should not be confused with developing an actual psychological profile

Search Engines

d0xing the Furneaux: The word d0x is a hacker term that means to work up a document on a target containing details about the target's personal life. Those details are often used to further attack the target, humiliate them, or perpetrate other crimes.

Webmii

Enter the Google

1. Search Engine Mysteries Revealed!: Search engines use little pieces of code called spiders. Spiders “crawl” through every web page on the open web and cache what they are allowed to access. There are certain files, like robots.txt, that stop a spider from indexing certain areas, but most other areas are indexed and cached
2. Enter the Operators: operators that limit what Google looks for.
3. But It Says “Private” Right in the Title: An RSA key is a key that is based on a proprietary algorithm. It comes in two parts: the public key, which helps identify it, and the private key, which unlocks the kingdom.
4. But It's Marked Confidential
5. Webcams: It's Time to Stop Dancing in Your Underwear
6. Other Sources of Intel: A webcam of some guy watching his marijuana plants grow People's private photos from their phones People's shared music and movie directories Documents containing full passwords, dates of birth, and Social Security numbers Thousands of credit card numbers in files Fully open SQL databases loaded with info Open access to traffic cams Open access to power grids and control systems A number of child pornography drop spots

Robots Are Cool

robots.txt file? It's a file that website owners use to tell the spiders or robots that crawl and scrape the sites what is and isn't allowable.
It's All About the Meta, Baby: metadata is literally data about data.

3 Profiling People Through Communication: (or Using Your Words Against You)

To effectively communicate, we must realize that we are all different in the way we perceive the world and use this understanding as a guide to our communication with others

1. There is always a source. There is a message. There is a channel. There is a receiver.
2. The Approach: Who are you? What do you want? Are you a threat? How long will this take?
3. Enter the DISC: D: Direct/Dominant I: Influencing S: Supporter/Steady C: Conscientious/Compliant
4. Your goal should be to keep the conversation focused on the person—not on yourself. By doing this, you will build trust and rapport, which makes your job as a social engineer easier.

4 Becoming Anyone You Want to Be

1. Pretexting is defined as the practice of presenting oneself as someone else in order to obtain private information
2. Principle One: Thinking Through Your Goals: Do you see how having specific goals changed my pretext for the better? Having the full details enabled me to develop a part of the pretext that helped me achieve all my goals without causing alarm. Powerful, right?
3. Principle Two: Understanding Reality vs. Fiction: My point is that your pretext should be based on facts, emotions, and knowledge that you already possess or can easily fake.
4. Principle Three: Knowing How Far to Go: Profiling People Through Communication": Who are you? What do you want? Are you a threat? How long will this take?
5. Principle Four: Avoiding Short-Term Memory Loss
6. Principle Five: Getting Support for Pretexting
7. Principle Six: Executing the Pretext
8. Do Not Use a Script

5 I Know How to Make You Like Me

Rapport is the ability to enter someone else's world, to make him feel that you understand him, that you have a strong common bond.

The Moral Molecule
The power of trust can make a person do something they instinctively know is not the best thing to do.
The 10 Principles of Building Rapport

1. Using artificial time constraints
2. Accommodating nonverbals

3. Using a slower rate of speech
4. Employing sympathy or assistance themes
5. Suspending your ego
6. Validating others
7. Asking how, why, and when questions
8. Making use of quid pro quo
9. Employing reciprocal altruism
10. Managing expectations

The Rapport Machine

1. Use the Friends and Family Plan
2. Read
3. Take Special Note of Failures

<u>6 Under the Influence</u>

1. Principle One: Reciprocity:
   Reciprocity in Action: Reciprocity works only when this path is followed. You can't interject the command or request too early
   Using Reciprocity as a Social Engineer: As a social engineer, it is imperative that you first find out what the target person or company values. You need to prepare your pretext with that in mind. When you offer the target a chance to have something of value, you are more likely to succeed. When you find what the person truly values, the target will grant the request you make with little to no thought.
2. Principle Two: Obligation
   Obligation in Action: Any time you don't, you reduce the chance of building rapport, because the target will be wondering why you didn't act "normal."
   Using Obligation as a Social Engineer: Obligation is a powerful principle that can make being a social engineer much easier.
3. Principle Three: Concession
   Concession in Action: If they can get a perp to admit to even a minor detail, to concede to one fact, it is nearly impossible for that person to go back on what he or she has said
   Using Concession as a Social Engineer: As a social engineer, remember that you don't need to go immediately for the exact flags you need. Get some minor ones to help build those feelings that will lead to the person to concede and comply
4. Principle Four: Scarcity
   As a social engineer, you can apply scarcity to time, information, or even things you are giving away in your pretext. Scarcity will make what you have more valuable and influence the target to make decisions based on that perceived value.

5. Principle Five: Authority
   But in Figure 6-6, he is standing with his chest out, hands steepled, chin up, and no look of fear in his face at all. All of this points to a person who is confident, and confidence makes us view the person as someone in authority. loud voice, chest out, chin up, neat clothes, direct personality, and other characteristics like that.
   Authority, even when it didn't come directly from me, made that security guard take an action that was not in his best interest. Authority is a powerful motivator!
6. Principle Six: Consistency and Commitment
   Playing the target's desire to remain consistent to their commitments, whether physical or mental, leads the social engineer to easier compliance with all the requests they make.
7. Principle Seven: Liking
   People like people who are like them. If you like someone, or make someone feel they are liked or trusted, that person can't help but like you.
   Liking is a powerful principle that can, literally and f iguratively, open many doors for you as a professional social engineer. If you are like me, the hardest part is learning to be interested enough that your "liking" comes off as genuine.
8. Principle Eight: Social Proof
   When we are lost, confused, or unsure, we generally look to others to see how they are acting for cues (social proof) for what we should be doing.
   More often than not, applying that slight social pressure worked —partially because people felt good about not being the f irst to give me all their information. Social proof has been one of the most powerful aspects of influence that I have used
9. Principles of Manipulation: Although they are negative, manipulation does have the following principles: Increased susceptibility Environmental control Forced reevaluation Removal of power Punishment Intimidation. Fear and anger override the brain's ability to think rationally, which leaves only emotion for making decisions.

<u>7 Building Your Artwork</u>

Art and science have their meeting point in method

The Dynamic Rules of Framing:

1. Rule 1: Everything You Say Evokes the Frame: Think about words you use in your daily vocabulary, and then decide if they might cause a target to feel one of the seven base emotions: anger, surprise, fear, disgust, contempt, sadness, or happiness. Then decide if that emotion is positive or negative. If it is potentially negative to a damaging degree, err on the side of caution before using the word.
2. Rule 2: Words That Are Defined with the Frame Evoke the Frame

3. Rule 3: Negating the Frame: If you don't want them to think about it, then don't say things like "I'm not gonna use it to hack you!" "It's not like I'm trying to break in!" "I would never send you a phishing email." "I'm not a crook!"
4. Rule 4: Causing the Target to Think About the Frame Reinforces the Frame: As a professional social engineer, you can reinforce frames by the words, clothing, and pretexts you choose. Keep the target thinking about your frame throughout your opening words, and it will make moving on to the next section so much easier. And we call that elicitation.

Elicitation

1. Ego Appeals: Appealing to the target's ego needs to be done with the following three things in mind: You have to use sincerity. You have to have the proper level of rapport. You have to be realistic. First, practice observing some things about people—let's say your family. "Hey, honey, you look super tired. Was your day okay?" A person's body language will soften. They will open up and become friendly and more talkative. Why? You validated them and appealed to their ego.
2. Mutual Interest: When your task is to social engineer someone or a group, and the topic may be challenging or the people may not be your favorite, look for the common ground. There usually is one thing that you can find that will allow you all to be on common ground and start a conversation.
3. Weather Especially if there is some odd weather—a heavy snow storm, too much rain, unseasonably hot or cold spells—the weather can provide quick opening topics to break the ice.
4. Technology Asking for advice on tech the target has (cell phone, laptop, smart watch, etc.) that you have observed can be a great way to get them talking.
5. Children As long as you ask questions at the appropriate level of rapport—and you are asking general questions about kids, not about their kids specifically— this can really get people talking.
6. Pets People love to talk about (and share photos of) their pets.
7. Sports Although not everyone is interested in sports, if you notice someone wearing a particular team's jersey or hat, it can be a great topic. As long as you don't say something like "Ah, Cowboy's fan, huh? Sorry."—which is not a very good opener.
8. I suggest you avoid topics like politics, health care, religion, other very deeply personal choices, or any violent news story. These topics can create a giant rift between you and your target.
9. Deliberate False Statement: We have the need to be right and to correct things that are wrong. When we hear something we "know" is wrong, we generally correct it, even if it is just in our own head first. Depending on who we are, where we are, and our passion for the topic, we might let the idea out of our head and into the open. But he went up to one complete stranger after another and threw out the weirdest deliberate false statements. Every time, people gave him information. The flaw with this method was there was no rapport. So, when he was done, his targets were left confused and wondering what had just happened. They definitely were not left "feeling better for having met him."

10. Using deliberate false statement too many times in a row can make you come across as unknowledgeable, and that can make your target lose faith in you. Don't confuse deliberate false statement with negating the frame. If you don't want the target to think about hacking, don't mention “hacking” in your deliberate false statement. Deliberate false statement works much better after you have built some level of rapport with the target. The deliberate false statement must have a ring of truth to it. If my student had approached the first woman and said, “Oh, you like strawberries—you must fly dragons,” he would have had nowhere to go with that; confusion would have been the result, not the need to correct.
11. Having Knowledge: The more believable you are, the easier it is for the target to assume you are who you say you are.

The Use of Questions: Questions are a natural part of conversation. From the moment we begin to speak, we use questions to send and receive data.

1. Open-Ended Questions: The words you use within a question elicit emotions, and those emotions affect the answer you get. An open-ended question encourages the target to engage their knowledge, attitudes, beliefs, opinions, and feelings. The success of these questions is largely dependent on the way you, as a professional social engineer, employ active listening and direct the questions to obtain useful information. This is important to understand, so when you are formulating your pretext, you can start to plan what type of questions you would naturally use. Remember, the goal is to keep the target talking openly about relevant details that can assist in the end goal of completing the social engineering engagement.
2. Closed-Ended Questions: Closed-ended questions elicit brief and narrow answers. Usually, they can be answered with one or two words. When you're using closed-ended questions, it's a good idea to start off with basic questions before getting to anything too deep. The basics of who, what, where, why, and how are good places to begin. Because of my perception of her confusion, I could add some facts that might not have been completely truthful.
3. Leading Questions: leading. I was led to focus on one thing and my brain blocked out everything else. As a professional social engineer, you have to plan ahead to be able to use leading questions. Build them into your pretext. Plan what you will do in order to lead targets away from the things you don't want them to notice.
4. Assumptive Questions: As a professional social engineer, assumptive questions can be used upon the initial approach in order to bypass certain conversation-stoppers. A conversation-stopper is just what it sounds like: a statement or statements that are made with the intent to stop someone from moving past a particular person or area

Summary

1. Each elicitation technique is an important part of a conversation. Learning how to use each can help you become a master at conversation and a superb social engineer. The goal of elicitation is to extract information in a normal-sounding conversation. If you practice these skills, that is

exactly what you will be able to do. The fascinating thing is that this is not limited to verbal conversations—these same skills work whether you are having a conversation over email, chat, text, phone, or any other means.

2. you can sprinkle a few questions into your conversation, add a dash of deliberate false statements, and mix in a healthy dose of mutual interest to elicit the information you need.
3. As you begin to master this skill you will be serving up perfect dishes of elicitation and conversation.

8 I Can See What You Didn't Say

It is our responsibility to learn to become emotionally intelligent. These are skills, they're not easy, nature didn't give them to us—we have to learn them.

1. Nonverbals Are Essential: It is important to understand how things work if I am going to truly help my clients. It is important to adapt and grow with new research. Sleep is really underrated. you can smell fear is actually true. Learn to control my fear so I can display the proper emotion. If that is not possible, build a pretext that uses my natural emotion.
2. Be Careful of Misconceptions

Know the Basic Rules

1. Rule 1: Focus on the What—Not the Why: Don't make connections between the what and why without having all the information. "Just because you can see the what does not mean you know the why."
2. Rule 2: Examine the Clusters: However, focusing on one cue is dangerous. You need context and other body language cues to indicate what is really being said. Look for matching nonverbal clusters that indicate what emotion is being displayed.
3. Rule 3: Look for Congruence
4. Rule 4: Pay Attention to the Context

Understand the Basics of Nonverbals

1. External stimuli come into our brain through our five modalities, assuming one is not damaged: sight, smell, taste, touch, and hearing. These stimuli are processed by our brains, and the stimuli can trigger one of the seven base emotions: anger, fear, surprise, disgust, contempt, sadness, or happiness. The emotion that is triggered creates physiological responses in both our faces and our bodies.
2. For example, when a person is confident, they make themselves bigger, which elevates testosterone and decreases cortisol in the blood
3. Creating the facial expression (even by force) creates the emotion associated with it. The key point to remember is that if you create an emotion, or you cause the target to express that emotion, you can leave the target feeling that emotion. You have to exercise caution when using this super power.

Comfort vs. Discomfort

Anger, Disgust, Contempt, Fear, Surprise, Sadness, Happiness

Summary

1. Foundational Tools As a starting point, this chapter can help you learn what subtle things to look for in the face and body for each emotion.
2. Better Understanding I hope you have a better idea of which emotions will work for you and how to not only see those emotions in others but display them yourself.
3. Defense Understanding how emotions are conveyed through facial expressions and body language can also be very helpful for you as a defense mechanism. Realizing how these emotions can and are being used will make you more aware when they are being used against you.
4. Enhancement As a professional social engineer, it is essential for you to always be learning and enhancing your skill set.

9 Hacking the Humans

If money is your hope for independence you will never have it. The only real security that a man will have in this world is a reserve of knowledge, experience, and ability.

SE over the last seven or so years: OSINT and how to use it, communication modeling, pretexting, rapport building, influence, manipulation, elicitation, and nonverbals.

The Principles of the Pentest

1. Information Gathering
2. Pretext Development
3. Attack Planning
4. Perform Attacks
5. Reporting
6. Information is the lifeblood of the social engineering attack. After you gather your OSINT, you can easily determine what pretexts may or may not work. Knowing how a company uses social media, communicates, is geographically located, and other details about their inner workings enables you to develop some good pretext ideas. After those ideas are developed, you can start planning the attack vectors. Will you send a phishing email? Or will you vish them for more info or credentials? Will you use a mobile-device attack? Will you go in person to the site? Will you combine those vectors? You can answer all these questions as you start to plan out the attacks. From there, you launch these attacks, collecting the results from all the steps and reporting to the client everything that took place.

principles of the SE pentest should include these points

1. Do you want to record phone calls? That is illegal in many states without consent
2. Do not just assume that the client should know exactly every step of a social engineering pentest.

3. Make sure you obtain written permission to record calls you will make. Many states are two-party consent, in which case, you will need to obtain the company's consent so you don't run into legal issues.
4. Detail the exact Google search string or tool that was used so the client can duplicate the steps if needed.
5. Don't live-tweet or post on social media about your successful exploits of your clients.
6. Document Everything
7. Be Judicious with Pretexts

Phishing

1. Educational Phishing
2. Pentest Phishing: aimed at obtaining remote access, credentials, or some other type of compromise.
3. Spear Phishing
4. Phishing Summary

Vishing

phishing over the phone

1. Credential Harvesting: vished credentials for VPN, email, secure storage, specific databases, and even door codes.
2. I tend to go with emotional pretexts that can offer the target the ability to “save” or “help” me. There is a science behind this. Giving someone the ability to trust you while you trust them with that role creates a very strong bond between two people. It releases oxytocin, and then that bond makes the target want to be consistent in their desire to help you, regardless of how insecure that decision might be.
3. For a professional social engineer, it is imperative to not be afraid of the phone if you want to succeed. Learn to embrace it, even if it is not your favorite method of communication. Having skill on the phone and learning to build rapport, gain trust, and then elicit information without being able to see your target makes you more successful.

SMiShing

1. Brevity is key. A SMiSh needs to be short and sweet— no build up, no opener and closer, just the facts and a link.
2. Links: then shortened URLs are way more acceptable in an SMS than in an email.
3. Don't skimp. If you are trying for credential harvesting, don't think that you don't need branding or the web page to look legit because the target is using a mobile device. To ensure you are fully testing targets, make sure to spend the time to make everything look real.
4. Don't make it too many steps.

Impersonation

1. A red team generally goes in at night (although it can be at any time) and focuses on trying to breach the physical security—elevators, locks, security cameras, and so on
2. Pretext Development: you need to consider some other things: clothing, tools, your look, and so on.
3. Attack Planning and Performing: Plan out what the attack should look like from start to f inish, and then make sure you have the tools on hand and tested to accomplish those goals.
4. a honeypot is a person who goes undercover to seduce another person into giving up sensitive information. It has also been used to describe a system (computer) that is set up to collect details from unsuspecting users.

All Details of Report :

1. how they found OSINT, the exact Google search string they used, or some other artifact
2. Being a professional social engineer is not just about being able to talk to others or being able to think quickly and clearly under pressure—it's about the whole package. Where are your weaknesses from this list: Elicitation Smooth talker Quick thinker Good report writer Professional speech

How Do I Get My Clients to Do SE Stuff?

1. Don't Offer Them Some of the Services for Free: when people pay, even a small amount, they add a value to it. If someone signed up and paid but didn't end up attending, they would be out the nonrefundable $50. That became a powerful incentive to attend. Don't think that giving away your talents for free will make people value you. It won't work. You can find the balance of offering a high-end service with some discounts or offering a three-month contract with one month free. It's okay to get creative about what you charge, but know that working for free just devalues your expertise.
2. Fail Fast and Move On

<u>10 Do You Have a M.A.P.P.?</u>

I'm a very big believer in controlling what you can, forgetting what you can't, and not wasting mental energy on things that don't deserve it.

1. Step 1: Learn to Identify Social Engineering Attacks: This first step of learning how to identify and know that these attacks exist will put your team light-years ahead of the average person. Help your employee population to understand the value of the information they possess—that emails can be used to breach the whole company; that phone calls are used to get passwords and other sensitive details; that if their mobile device is breached, it can be used to attack their home and work networks; and that just because a person is smiling and friendly, you can't ignore the badge policy. Apply that and learn from it. Don't assume that the knowledge about these attacks is just common sense. When someone doesn't have the knowledge, it doesn't mean they're just stupid,

lame, and deserve to fail. Instead, have empathy and think: “Okay, we can do better next time. How can we do that?” That will really help you make the next step more successful.

2. Step 2: Develop Actionable and Realistic Policies : “Check all IDs,” is not enough, because when empathy kicks in, that good ol' amygdala shuts down logic centers so that people make decisions solely on emotional thoughts. The education, reminders, and clear instruction help remove the empathy bypasses and ensure secure process.
3. Step 3: Perform Regular Real-World Checkups
4. Step 4: Implement Applicable Security-Awareness Programs
5. Each of these stories contains details about a breach, how it occurred, what caused it, and what vulnerability was exploited (whether it was human, hardware, software, or all of these). Understanding attacks that affect other companies can help your company stay safe

Create a Security Awareness Culture

1. Rewards
2. Positive Reinforcement
3. Extra Training

11 Now What?

It's easier to limit yourself, but if you do, you will never reach your true potential.

1. Soft Skills for Becoming an Social Engineer: Humility, Motivation , Extroverted, Willingness to Try
2. Technical Skills: Understanding how to use simple technology, such as USB keys, booting machines, and connecting to a VPN, can go a long way in helping you with your pretexts and after you gain access. Basic computer knowledge Basic office productivity knowledge (such as Word and Excel) Knowledge of the different parts of a computer and how they operate Ability to navigate in Mac, Windows, and Linux operating systems Understanding of how a network works Knowledge of how to set up a mail server Photo-editing skills. exploitation in your pentests, you also need the following skills: Knowledge of exploit frameworks like Metasploit and Empire Ability to read and understand code Ability to write some code
3. Education: Psychology, Language, Grammar, and Writing, Social Psychology
4. Job Prospects: Start Your Own Company, Speak at a conference, or write a few blog posts or articles and get people to read them and comment on them. Having even a small public name in this space can help make your business a valid contender for providing services. I have seen a few people start a successful business by generating some buzz in the community even though they had no previous experience in social engineering. They came to DEF CON and entered the Social Engineering Capture The Flag (SECTF) contests I host there. After doing really well and winning, they went on to create successful companies that provide social engineering services. Building

credibility helped them along their path., Get Hired by a Pentest Company, Get Hired by a Social Engineering Company

5. The Future of Social Engineering: People who join terrorist groups are angry, emotional, and looking for a tribe. Then a tribe comes along and gives them answers and motivation to "solve" their problems. The people feel needed, wanted, and accepted. The new tribe asks for small things at first, building trust and a close bond. This continues until the conversion is complete.