467.1

Social Engineering Fundamentals, Recon, and Phishing

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

SEC467.1 | Social Engineering for Security Professionals

SANS

Social Engineering Fundamentals, Recon, and Phishing

Welcome to Security 467, "Social Engineering for Security Professionals." The course authors for this class are Dave Shackleford and James Leyte-Vidal. The focus of this class is to build your social engineering skills as a component of effective penetration testing, both in terms of principles of persuasion and technical skills.

We welcome feedback about this class; please send it to us at dshackleford@sans.org and jameslvsec467@gmail.com.

Course Outline

- Section 1
  - Introduction to SE Concepts
  - The Psychology of Social Engineering
  - Social Engineering Goals
  - LAB: Setting up for Success
  - Targeting and Recon
  - LAB: Recon and Profiling Exercise
  - Secure and Convincing Phishing
  - Tracking Clicks
  - LAB: Tracking Clicks
  - Secure Phishing Forms
  - LAB: SET Site Cloning
  - LAB: Data Logging

The slide above outlines the topics covered in this course. To apply social engineering effectively in penetration testing it is important that you understand both a number of psychological principles and also technical methods. We focus on how to emulate the techniques attackers use to cheat their way into obtaining data. We also look at a practical set of techniques, such as measuring the victim click rate for your reports.

Social engineering can be a tricky business that can touch on matters of ethics, law and how clients (or your company) may try to punish people based on your work. As much as possible, we share our experiences throughout the course and provide you with advice that may help you avoid similar challenges. Social engineering is a space powered by creativity and innovation, and we have no doubt you will be able to build on what we tell you and come up with new variations or cool tools to help you and your community. With that in mind, we next introduce the core concept of social engineering.

In this section we take a look at the fundamentals behind social engineering, some of the psychological factors of social engineering and what makes good social engineers so successful. Then we look at the goals of social engineering, merging the technical focus for pen testers with the results of the business needs.

After talking about the psychology and goals of social engineering pen tests, we get into the tactical side of things. First, we spend a lot of time on target profile development and information acquisition. Many pen testers will be familiar with the concept of "recon," especially using open source techniques, but we're going to take it to a whole new level! Once we've built our target profiles, we'll begin looking at actual testing techniques, starting with phishing. Phishing is one of the most common and popular types of SE pen testing, but there are a lot of tools and tactics you can employ to ensure that your campaigns are successful.

Introduction to Social Engineering Concepts

This section kicks off the course with a discussion of social engineering concepts that serve as the background for penetration testers who plan to perform social engineering exercises.

What Is Social Engineering?

"In the context of information security, social engineering is the **psychological manipulation** of people into **performing actions** or **divulging confidential information**. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of **confidence trick for the purpose of information gathering, fraud, or system access**, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Source: Wikipedia

It's always helpful to start off with some definitions. So, what exactly is social engineering? In a nutshell, it's the manipulation of people to gain access to data and information, often with a secondary goal of gaining systems or data access. Social engineers use trickery and deception to solicit needed information from targets, allowing them to achieve their goals of compromising an organization's or individual's systems or facilities in some way.

It's worthwhile to dissect this definition a bit more. For pen testers, the goal is to find and demonstrate vulnerabilities that may be present within an organization, whatever form those vulnerabilities may take. In the case of social engineering, we're seeking to demonstrate the following:

- A lack of proper security awareness, and potentially gaps in the current model/content of security awareness training being offered to employees and other relevant stakeholders.
- The kinds of information users may be willing to divulge, and what they're capable of divulging.
- How end user compromise can subsequently lead to other security breaches or scenarios.
- Where/How existing security controls and processes are failing, and what can be done to improve them.

Social engineering, in various ways, leverages **psychological manipulation** to accomplish these goals.

Source: http://en.wikipedia.org/wiki/Social_engineering_%28security%29

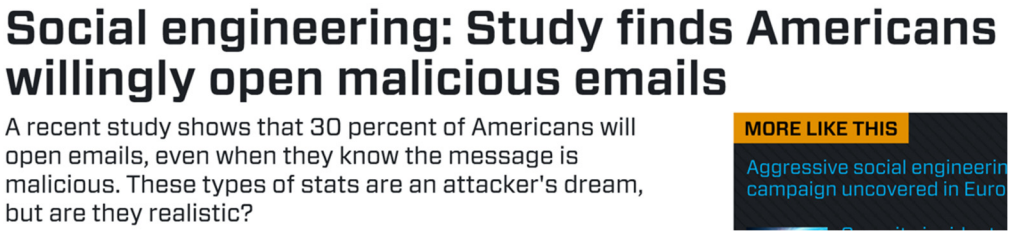
Kevin Mitnick was likely the most famous social engineer in the world for quite a long time (or at least one of them). He's been in plenty of trouble for his exploits over the years, actually serving jail time, but he is now a consultant who performs penetration tests and trains organizations to combat social engineering attacks. In his book *The Art of Deception*, Mitnick describes social engineering as follows:

"*Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."*

This description of social engineering nicely complements the one we just discussed, as it ties into the motivations and methods that a social engineer may take to accomplish his or her goals.

Social Engineering Today

- Social engineering is a very common tactic in attacks today
- Consumers and business users are susceptible to these attacks



There are many cases of social engineering being used today. According to a 2013 study conducted by TNS Global and e-mail security company Halon, 30% of Americans willingly open malicious e-mails—even when they know they're malicious! Although this sounds insane, there are definitive psychological trends and patterns that contribute to this, which we cover shortly.

Many more studies and examples have shown this since, as well. Some other interesting statistics include the following (source: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html):

- 94% of malware is delivered via email
- Phishing attacks account for more than 80% of reported security incidents
- $17,700 is lost every minute due to phishing attacks

Although consumers fall prey to this constantly, what many studies are finding is that these same people are just as vulnerable in the workplace. This is a disturbing trend that security teams are fighting to address, and social engineering pen tests can help to highlight where an organization needs to spend more time on security awareness training.

Image and article source: http://www.csoonline.com/article/2133877/social-engineering/social-engineering--study-finds-americans-willingly-open-malicious-emails.html

Attacker Trends: The Last Decade

- Attackers are wising up to social engineering tactics and getting more sophisticated
- Advanced attackers:
  - Build target profiles
  - Send highly targeted phishing e-mails
  - Leverage media drops and pretexting
  - Execute complex SE campaigns

In the popular media today, many are led to believe that Advanced Persistent Threats (APTs) are commonplace, where attackers are so advanced and sophisticated that they are releasing 0-day vulnerabilities in every reported breach and using incredibly high-end methods to break in and achieve their goals. This could not be further from the truth.

Many of today's most high-profile breaches, in fact, start off with social engineering, sending targeted phishing e-mails or using pretexting phone calls to convince targets to download content, visit a site or take some other action that gives an attacker an initial foothold on their system(s). The most advanced attackers often invest a lot of time in social engineering campaigns, some of which may involve cutting-edge exploits or malware. Today, with more and more organizations patching their external-facing systems, the easiest way in may very likely be through social engineering.

Case Study: RSA (1)

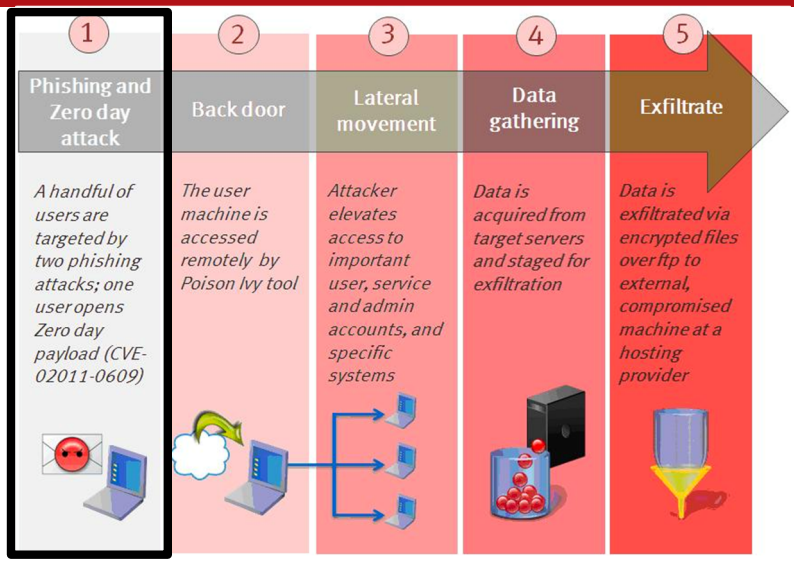
- RSA employees were targeted with spear phishing and clicked on an Excel spreadsheet attachment
- A Flash 0-day exploit was in the spreadsheet
  - This led to the breach over time

RSA

One of the most high-profile breaches in the past ten years, the attack against RSA, illustrates how any high-profile technology company (especially a security company) can come under fire from advanced attackers. In this case, the attackers gained access to RSA's network through a phishing attack, then dropped a 0-day exploit on employee desktops through an Excel spreadsheet that employees opened. The attackers gradually moved through the RSA network, looking for (and finding) sensitive seed files for RSA's encryption algorithms used in their popular 2-factor token solutions. These seed files were then leveraged later for attacks against defense industrial base companies like Lockheed Martin and others.

The entire breakdown of the attack is chronicled here: https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/.

Case Study: RSA (2)

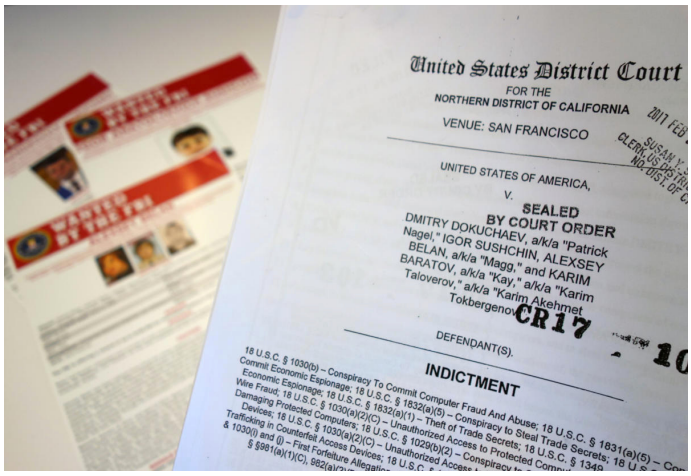


This slide shows the RSA analysis of the attack against them. Note the first phase on the left side of the diagram, which demonstrates that the attack started with phishing and a 0-day exploit. Many attacks today originate with phishing, both targeted and general purpose. As pen testers, we need to use the same tactics the attackers use.

Image source: https://blogs.rsa.com/anatomy-of-an-attack/

Social Engineering Breach: Yahoo

- In 2016, Yahoo announced a major breach of account data
- The breach involved spear phishing against Yahoo admins
- A total of over a billion accounts were compromised in total



In 2016, Yahoo announced a significant breach of over 500 million accounts that had apparently taken place starting two years earlier in 2014. The US FBI got involved and assisted in the investigation to help Yahoo determine what had happened and the full scope of the breach.

During the investigation, it turns out that Russian state operators were targeting a number of specific Yahoo accounts and hired several highly skilled hackers to break in and locate account data. These attackers gained initial entry through targeted spear phishing emails sent to privileged admins at Yahoo, and then pivoted from the admin systems to other parts of the Yahoo network (a common and familiar tactic). Backdoors were enabled for repeat access, and additional details that emerged point to billions of accounts possibly affected.

Image source: https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html

Social Engineering Breach: Twitter

- In 2020, a number of high-profile Twitter accounts were hacked and began asking for Bitcoin payments
  - Accounts affected included Elon Musk, Bill Gates, and Barack Obama
- The attackers targeted Twitter admins via pretexting phone calls, masquerading as IT admins
- The attackers did research on LinkedIn and other sites to specifically target new and inexperienced employees

Several Twitter accounts started sending out very unusual requests for Bitcoin donations in July 2020, including Jeff Bezos, Bill Gates, Barack Obama, Joe Biden, and many more.

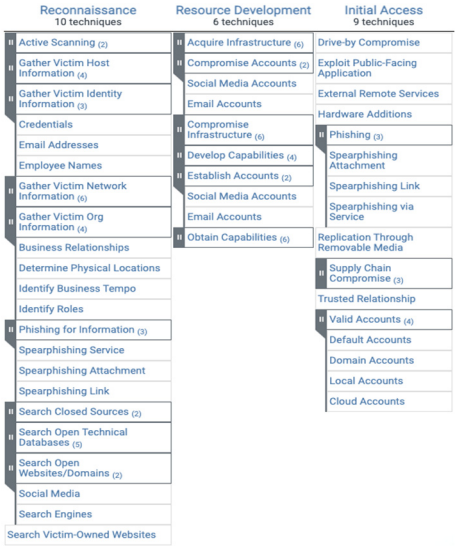
Twitter quickly froze the accounts in question, but the investigation revealed a significant compromise of over a hundred high profile accounts, and some accounts' personal data had apparently been accessed and exfiltrated from the Twitter environment, as well. Twitter acknowledged early on that a targeted social engineering campaign had been involved against employees, but the later stages of the investigation showed that the attackers had very specifically targeted new and less experienced employees with phone-based pretexting (covered shortly) requesting them to enter credentials into a fake site. While the employees entered the credentials, a phone-based multifactor request came to the employees, some of whom entered this, too, allowing the attackers to gain access.

These employees' systems provided enough data and information to target higher-ranking employees successfully and take over Twitter account management tools.

Image source: https://www.news18.com/news/tech/twitter-hack-breach-compromises-many-public-figures-including-musk-obama-twitter-investigating-incident-2717995.html

Attack Frameworks: MITRE ATT&CK

- Reconnaissance:
  - Look for accounts/identities
  - Look for credentials
  - Phishing
  - Evaluating business relationships
- Resource Development
  - Accounts and Email
- Initial Access
  - Phishing
  - Account compromise



One attack framework that has emerged in recent years is the MITRE ATT&CK model that describes detailed stages of many common attacks, including social engineering.

Some of the stages and categories include

Reconnaissance
- Searching for online account and social media presence that may represent fruitful targets
- Searching online for credentials that may be useful (possibly from previous breaches or accidental exposure)
- Phishing for information (similar to the Twitter breach of 2020)
- Looking for business relationships and other relevant information to craft believable attack context

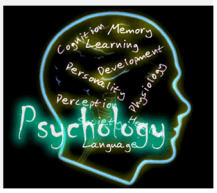
Resource Development
- Developing false profiles and accounts, or even entire web sites, that can be used during social engineering attacks

Initial Access
- Sending targeted phishing emails with malicious links or malware
- Compromising accounts through credential hijacking or other methods

The framework is updated often, and any pen testers should use the model's attack patterns to help craft targeted exploitation attempts.

Image source: https://attack.mitre.org/#

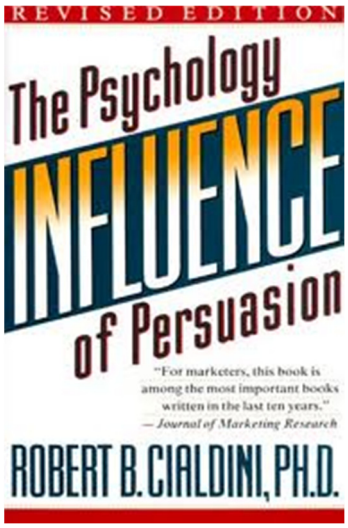
The Psychology of Social Engineering



In this section, we cover some of the key psychological principles to keep in mind for social engineering. Although this is not at all an in-depth treatment of the psychology of persuasion and human manipulation, the key points will be important to understand for any pen testers looking to be successful in various SE campaigns.

The Principles of Persuasion

- Dr. Robert Cialdini first posited the major motivations and incentives for human persuasion years ago
- Why do people act the way that they do?
- This is the basis for why social engineering works



Robert Cialdini is believed by many to be the "father" of human persuasion research, which is directly related to the activities involved in social engineering. Dr. Cialdini studied many different types of human behavior but focused on the attributes of human nature that were most prone to manipulation. In his seminal work *Influence: The Psychology of Persuasion*, Dr. Cialdini lays out the major principles that form the basis for much of how we influence people today. This applies to *all* types of influence, ranging from the saleswoman who knows how to get a successful contract, to an employee who is negotiating for a raise, to a social engineer who is trying to get you to click on a link or give up personal information over the phone.

Over the next several slides we discuss Dr. Cialdini's work from the perspective of the professional social engineer. He's come up with six principles that tie into human behavior patterns related to persuasion—what makes people tick? How can they be persuaded to give up information to a social engineer? How should social engineers behave and what ideal characteristics should their campaigns include to maximize susceptibility to SE? Let's explore the real psychology behind social engineering now.

Principle #1: Reciprocation

- People feel indebted when someone does something for them
- How does this work in social engineering?
  - Holding the door for people
  - Classic spam campaigns (Nigerian prince)
  - Appealing to ego ("Please speak/participate")
  - Giving away a USB or token "gift"
- The "Chocolate for Passwords" experiment

The first principle that Dr. Cialdini describes is "reciprocation." In a nutshell, people feel indebted when someone does something for them, and they will often provide information or perform some token activity to pay off the "debt." There are many nuances to this principle. First, the perceived debt does not even have to be realized—just the offer of something nice is often enough to create a mental debt. Second, what the SE asks for must be proportional to what is given or offered. You can't offer to hold the door for someone and then expect them to give you their bank account number. You can, however, expect that they'll hold a second door for you in return (in some cases) or something similar.

This technique is used by social engineers and criminals alike all the time. One of the most well-known examples of this principle in action is the classic "Nigerian prince" spam campaign. An e-mail arrives, purporting to be from a Nigerian (or other) monarch who has been put in the unfortunate position of having to move a large sum of money out of his/her country quickly. This person needs the help of the recipient, who should provide banking details to move the money into, for which they will be compensated with a sum or percentage of the money being moved. They ask for help but giving you money makes you feel indebted to do so. Of course, there is no money or monarch—this is just a scam to get bank details. It must be working on *someone*, though, as it continues to be seen in the wild. More subtle examples that work in social engineering exercises include appealing to someone's ego or giving them a small gift or token. The first example may take the form of a tailored e-mail that asks if the target is interested in speaking at a conference or participating in a prestigious event of some sort. To find out about it, they'll need to click a link or open an attachment. The second could happen at a trade show, where a vendor gives away a free USB drive but requires your e-mail address and contact information for follow-up before providing it.

A great example is an experiment done in 2004 in the UK, where researchers offered a piece of chocolate to commuters who would give away their passwords. Over 70% complied: http://news.bbc.co.uk/2/hi/technology/3639679.stm.

Principle #2: Social Proof

- When people are uncertain about a course of action, they tend to look to those around them to guide their decisions and actions
  - The "follow the herd" or "fitting in" mentality
- Applicability to social engineering:
  - E-mail spoofing (trust issues)
  - Installing apps that others use
  - Group norms (smoking outside, etc.)
- Personalization is the key to this method

The second principle that Cialdini describes is one he calls "social proof." In essence, this concept relates to how humans tend to look for reassurance when they don't know how to act or respond. Most people will behave as others do if they're part of the same peer group and will especially mimic behaviors when they're exhibited by leaders or those in positions of power or authority.

For example, e-mails that entice a user to perform some action (clicking a link or opening a file, for instance) could be spoofed to look like someone in the target's peer group or some other associated group, which may increase the likelihood of the attack succeeding. If others in the peer group or an associated group are all using a certain application or technology, a targeted attack that uses "peer pressure" to use the same technology or app (with a supposed link to the app in an e-mail, perhaps) may be more successful. Group norms, like smoking outside or visiting a certain coffee shop nearby, can also be used to target and compromise a victim.

This method needs to be personalized, which means doing some homework for the pen tester. In order to create convincing coercion techniques from peers, friends, and other associates, pen testers need to learn about them and their behaviors.

A great video entitled "Social Conformity – Brain Games" can be found at https://www.youtube.com/watch?v=o8BkzvP19v4

Principle #3: Commitment and Consistency

- We're more likely to do something after we've agreed to it verbally or in writing
- The older the person, the more this holds true as well
- Applicability to social engineering:
  - Multi-part attacks (first, request; then, follow up)
  - Longer-term influence on behavior
- Kevin Mitnick used this to great effect

The third Cialdini principle is commitment or consistency. If someone agrees to do something verbally or in writing, they're much more likely to follow through with it. This doesn't have to happen all at once either—small and incremental agreements to do things can ultimately lead to an attacker asking for a larger commitment, which may then happen. Usually, asking for a large commitment immediately may arouse suspicion, so careful attackers need to ask for a small commitment (clicking a link) or work up to a larger commitment (giving away sensitive data).

Consistency is just a human trait. We tend to follow patterns daily. We tend to park in the same spot if possible, every day, eat at some of the same restaurants, and take a cigarette break at the same times. Attackers can learn these patterns and potentially exploit them. Kevin Mitnick was famous for this style of attack. He would call people on a regular basis (building *consistency*) and then gradually ask for favors. Eventually, he'd get what he wanted from them.

Principle #4: Liking

- People prefer to say "yes" to those they know and like. People are also more likely to favor those who are physically attractive, similar to themselves or who give them compliments
- Applicability to social engineering:
  - Look the part. "Fit in".
  - Most applicable for on-site work, but can be applied to e-mails, etc.

This one is pretty easy to understand—people tend to like people they're attracted to or to those who are similar to them in some ways.

To make use of this Cialdini principle, pen testers need to establish some rapport with targets. As this is one of the most effective techniques for successful social engineering, the key to getting people to like you is to do some research on their hobbies and interests and echo them back. This takes practice. You can also compliment people, but this is an art, as too much complimenting will actually lead to the target becoming suspicious or tuning out the attacker.

Although it sounds cliché, sometimes the key to getting people to like you is to be as much like them as possible. This may mean dressing a certain way, acting in a certain manner, or using a particular type of language.

Principle #5: Authority

- People respect authority. They want to follow the lead of real experts.
- Business titles, impressive clothing and even driving an expensive, high-performing automobile are proven factors in lending credibility to any individual
- Applicability to social engineering:
  - Send e-mail from an authority figure
  - "Look the part"

Cialdini's fifth principle is that of authority. This takes a bit more finesse for pen testers. Overt authority plays can actually backfire in many Western cultures. For instance, calling a target and saying, "Hi, I'm your boss's boss's boss, now give me this user's password!" will fail miserably. However, there are many ways to subtly leverage the principle of authority. For instance, dressing well or driving a nice car may easily impress people, leading them to believe that you are an important person. This can easily get you past a secretary or other "guardian" in some cases.

For phone calls and e-mails, the language you use and the way you present the case scenario may have an impact on the target. A subtler approach may work. In fact, some of the most successful social engineering attempts are those that indirectly reference authority—for example, "My boss needs X before the end of the day…can you help?" In this case, the mention of authority figures imposing deadlines may sway the target—who doesn't understand an overbearing boss who demands things in short order?

Principle #6: Scarcity

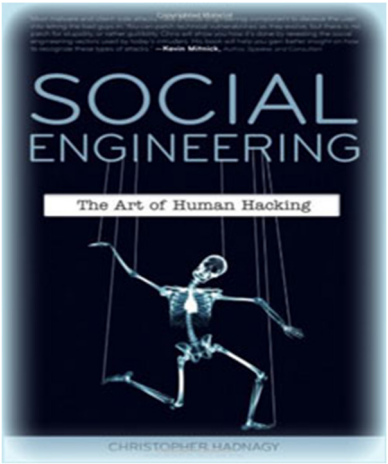
- The less there is of something, the more valuable it is
- The more rare and uncommon a thing, the more people want it
- Applicability to social engineering:
  - Make links and sites attractive with terms such as:
    - "Don't miss this chance…"
    - "Here's what you'll miss…"

The Cialdini principle of scarcity is easy to understand but harder to execute in social engineering attempts. Everyone wants something that others have when they do not. This can easily be exploited with some finesse. For example, an e-mail that offers a "limited time offer" or "Apple products before official release" can get significant interest, even if we know this sounds hokey.

A related tangent to this is simply time pressure. Sometimes, people need to be enticed or pressured to perform some action in a short time frame. Depending on the scenario, reward or punishment can be used to lure targets to perform the action desired.

Five Fundamentals

- Chris Hadnagy described five fundamentals of influence and persuasion:
  - Setting clear goals
  - Building rapport
  - Being observant of your surroundings
  - Being flexible
  - Getting in touch with yourself (emotions)
- These are all key to a successful SE engagement



Chris Hadnagy, a world-famous social engineer and physical pen tester, authored a fantastic book aptly titled *Social Engineering: The Art of Human Hacking*. In his book, Hadnagy describes five key principles of influence and persuasion that align well with the classic Cialdini foundation. These include the following:

- **Setting clear goals**: When setting out to social engineer someone, have a plan in mind. For example, don't just show up on-site at a target location and hope for the best. Know that your plan is to get inside a certain area, tailgate employees at a particular entrance, etc.
- **Building rapport**: Building rapport with people is the key to getting what you want, which is *always* a goal in social engineering! We'll talk more about this later in the class.
- **Being observant of your surroundings**: Especially for on-site social engineering, you need to pay close attention to people, behaviors, site-specific circumstances, etc. For example, let's say you have done the proper recon on a physical location and know where you want to tailgate. When the time comes to make an attempt, two police cars pull up right in front for something totally unrelated. In this case, it's best to wait or attempt an alternative approach versus blowing your cover.
- **Being flexible**: Never have only one approach! Successful social engineers know that being flexible with people and changing circumstances is key to accomplishing your goals.
- **Getting in touch with yourself (emotions)**: Although this sounds wishy-washy, it's actually a very simple principle. Everyone is different, including social engineers. Know your own tendencies and habits and accommodate for them during engagements. For example, if you have a hyperactive personality, but you are attempting ingress to a very calm and relaxed office environment, you'll need to take pains to calm down and appear mellow before entering.

Social Engineering Planning

- Successful security operations teams will carefully plan all social engineering activities
- Planning for social engineering includes the following:
  - Scope of the engagement
  - Terms of engagement
  - Covering your bases legally
  - Defining proper goals for the engagement

For social engineering assessments, planning is key! Any good social engineering assessment will include a number of distinct planning components, all of which we'll cover in more detail in upcoming slides.

First, you need to define scope. What is the test going to consist of, and who/what is covered?

Next, you need to ensure you've defined the terms of the engagement. How will the test proceed? What logistics and particular coordination steps are required by the client or your internal stakeholders?

Third, you need to cover yourself legally. This is a very sensitive type of engagement that can result in conflicts and even law enforcement involvement if not managed appropriately.

Finally, what are the major goals of the engagement? Understanding this is absolutely paramount.

Let's dig into these areas of focus.

Defining Social Engineering Scope

- The first thing to discuss with stakeholders is the social engineering scope. This can include:
  - People to e-mail for phishing
  - Numbers to call for pretexting
  - Specific phishing/pretexting models or templates
  - Locations for on-site social engineering
  - Payloads/execution models for USB and phishing tests

Defining the scope of a social engineering test is a critical aspect of "getting it right." The scope, in essence, is the "what" and "who" of a social engineering pen test. Depending on the type of engagement, the client or stakeholders may have this explicitly defined, or you may need to help them define it. Here are some key things to discuss and nail down:

- If phishing tests are included in the engagement, which people will be included? For spear phishing, in particular, what people will be targeted? The total number of e-mail addresses to include in the test(s) should also be discussed.
- If pretexting (phone-based social engineering) is to be performed, what numbers will be included and who will be called? How many calls will be performed?
- In the scope, it's common to define the particular types of phishing or pretexting models that will be employed during the test. In many cases, some of this could be "TBD" and coordinated in real-time when the test comes about. For other engagements, you'll have very particular requirements defined. For example, "accomplishing a password reset with the help desk" is a common pretext. A common phishing template might include "updating your healthcare plan information."
- If on-site physical social engineering will be performed, at what sites will it be done?
- If media drops are to be included (DVDs or USBs, for example), how many will be dropped and where? Also, what types of payloads or execution models are in scope for different locations?

Scope and Terms of Engagement

- In addition to the scope, you'll simultaneously need to define the terms of engagement. This includes:
  - Testing start and end dates and times
  - Post-exploitation activities
  - "Click and track" or "exploit and pivot?"
  - USB payloads
  - Contact information and coordination
  - Discussion of sensitive data exposure

In most cases, you'll want to define both scope and terms of engagement at the same time. Where the scope is "who" and "what," the terms of engagement are all about "how" and "when."

Some of the major things you'll need to nail down in defining the terms of engagement include the following:

- **Testing start and end dates and times**: When will the test be kicked off? When does it end? Also, does the client have particular times of day when the test needs to be conducted? Clients often have concerns about certain types of testing during production hours or want to avoid known busy times for support teams.
- **Post-exploitation activities**: If you do have permission to actually exploit users during the engagement, how far can you go? This starts to delve into more expansive pen testing activities, which are better covered in the SEC560, SEC542, SEC642 and SEC660 courses.
- **"Click and track" or "exploit and pivot"**: For phishing tests in particular, what is the approved delivery model and exploitation activity? Are you only tracking user clicks? Or are you actively dropping payloads and exploiting endpoint systems?
- **USB payloads**: If USB or other media drops are included in the testing, what types of payloads are in place? This is really the same issue as just mentioned for phishing—do you simply track clicks or attempts to open a file, or do you actively look to exploit the endpoint?
- **Contact information and coordination**: Ensuring that you have the right contact names, numbers, and e-mail addresses for target personnel is crucial. If something goes wrong, or you get apprehended on-site, you'll want to ensure you have the appropriate contacts in place. In addition, discuss the timing and frequency of coordination efforts—will you have a daily or weekly status call? What kind of status information is requested?
- **Discussion of sensitive data exposure**: If the possibility exists that sensitive data may be exposed during the engagement, then you may need to complete a "data transfer" agreement that stipulates how any personal or protected information is handled and disposed of.

Terms of Engagement: What Changes with SE

- People are involved!
  - There may be significant privacy ramifications
  - Access to personal (non-work) data is also a possibility
- Some SE projects bring new risks:
  - Police and law enforcement
  - Armed personnel
- Some SE projects also require specific engagement strategies:
  - "Don't get caught," for example

Many things about social engineering tests differ from traditional pen tests. First, you are guaranteed to interact with people, so you'll need to be cognizant of personal or private data that may be exposed during the test. If a target user finds a USB in the lobby and brings it home to plug in, what happens if the system he plugs into is a personal one? You'll need to plan for these types of contingencies at the beginning of the test.

If you are going to perform physical tests on-site, ranging from tailgating to planting credit card skimmers and wireless access points, there is a strong likelihood that law enforcement may get involved at some point. This is certainly a new risk, and most pen testers won't want to spend a night in jail while the details get sorted out! We cover this more in just a moment. What about armed target personnel or hired security guards? This brings additional risks, obviously!

Depending on the goals of the test (covered shortly as well), you may need to adopt new terms of engagement and wholly different strategies for the test. For example, one type of test that is commonly employed is avoiding detection or capture while on-site. To accomplish this, testers may need to be especially stealthy and spend additional time performing recon activities to better understand the nature of the target environment and people before attempting penetration efforts.

Social Engineering Strategy

- Strategy will depend on the overall goals of the assessment and testing types
- The key considerations include:
  - Scope and terms of engagement
  - Types of testing
  - Pen testing goals
  - Budget and cost
  - Time
  - Geographic locations (maybe)

At this point, it's prudent to take a step back and recap, while also discussing the "big picture" strategy of the assessment. Defining the scope and terms of engagement is an important exercise but there's much more to properly planning and executing a social engineering test. What types of testing will be involved? This, of course, is a major focus for the class, and we'll be covering different testing methods and focal areas shortly. Aligning with the types of testing are the target organization's goals for the test in general—do they need to gauge the effectiveness of their security awareness program? Do they want to see how vulnerable their physical locations are to unauthorized ingress attempts? We cover some of the more common goals in just a bit.

Budget and cost play a big role in what an organization can hope to accomplish in a social engineering pen test. Planning and recon take time, as do execution and reporting. You'll need to accurately determine how much time to spend on each task and that will be subjective based on your skills, tools, and ability to execute. We'll certainly help with some of that in this class but there are always factors that are individual in nature too. The amount of time you have to perform the activities may also be dictated by how many team members you can spare at the same time. If you'll be on-site, where those physical locations are can easily dictate schedules and approach.

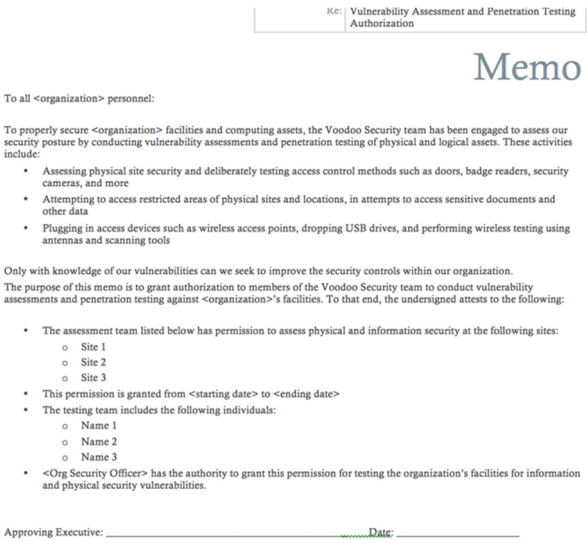
Get Out of Jail Free

- You must get a signed statement of permission to test anyone's people, systems, or applications!
  - Often called the "Get Out Of Jail Free" memo, or GOOJF
- Some organizations will accept an email or other form of "proof" in this regard for remote testing
  - A signed letter/statement is best for in-person tests, however

While planning your pen test, you'll need to ensure that you are legally covered with a Get Out Of Jail Free card/memo, or GOOJF. This is a signed statement from the target organization that absolves you and your team of liability for performing penetration testing activities, which, in many cases, are illegal or at least highly suspect. In short, don't perform *any* types of penetration testing without having a GOOJF statement that is signed and accepted by the top level of executive you can get to at the target organization.

Ed Skoudis has a great sample memo at www.counterhack.net/permission_memo.html that has been adapted for use by many SANS students. Another example is provided on your course USB, courtesy of one of the course authors who uses variations of this in engagements today.

Example: No Jail for You!



Re: Vulnerability Assessment and Penetration Testing Authorization

Memo

To all <organization> personnel:

To properly secure <organization> facilities and computing assets, the Voodoo Security team has been engaged to assess our security posture by conducting vulnerability assessments and penetration testing of physical and logical assets. These activities include:

- Assessing physical site security and deliberately testing access control methods such as doors, badge readers, security cameras, and more
- Attempting to access restricted areas of physical sites and locations, in attempts to access sensitive documents and other data
- Plugging in access devices such as wireless access points, dropping USB drives, and performing wireless testing using antennas and scanning tools

Only with knowledge of our vulnerabilities can we seek to improve the security controls within our organization.

The purpose of this memo is to grant authorization to members of the Voodoo Security team to conduct vulnerability assessments and penetration testing against <organization>'s facilities. To that end, the undersigned attests to the following:

- The assessment team listed below has permission to assess physical and information security at the following sites:
  - Site 1
  - Site 2
  - Site 3
- This permission is granted from <starting date> to <ending date>
- The testing team includes the following individuals:
  - Name 1
  - Name 2
  - Name 3
- <Org Security Officer> has the authority to grant this permission for testing the organization's facilities for information and physical security vulnerabilities.

Approving Executive: _____ Date: _____

This slide shows a screenshot of the memo in your media files, which your instructor may walk through briefly in class.

General Tips from the Trenches

- Be explicit—don't assume anything
- Get your GOOJF handled early
- Understand where and whom you're testing
  - What data types will you encounter?
- Prep work ALWAYS takes longer than you think
- Build in more time for on-site work—ALWAYS
- More advanced tests will require more recon

To finish up the planning section of the course, here are a few additional "tips from the trenches" that should be top of mind when planning any social engineering pen test project.

- **Be explicit and don't assume anything**: Make sure when planning a social engineering test that you get exact requirements from the target personnel. Don't assume something is in scope or that a certain type of testing is okay. Get it defined precisely upfront.
- **Get your GOOJF handled early**: Sometimes politics and bureaucracy can hold up the issuance of the GOOJF memo; plan for this and get it done very early.
- **Understand where and who you're testing**: Make sure you know the laws and legality of who and where you are testing. What data types may you encounter? This is very important to prevent accidental violation of laws and/or policies.
- **Prep work ALWAYS takes longer than you think**: Account for the amount of prep and recon time you will have to do. In most social engineering tests that involve anything more than sending out a generic phishing blast, there is time needed to learn the people, the organization, the culture and also to configure tools and set up the campaigns. Do not underestimate how much time all this can take!
- **Build in more time for on-site work—ALWAYS**: on-site work always has hiccups or unanticipated events. You may encounter a security system you did not know about. You may find yourself much MORE successful than planned and you will need more time to dig in and exploit things. Whatever the case, make sure you have enough time planned, or that you and the client/target have negotiated "ad hoc" additional hours and time if it's discussed and warranted.
- **More advanced tests will require more recon**: We cover recon momentarily, but for now, know that any test looking to emulate advanced attacks or scenarios will require significant time for learning the various aspects of the organization.

Lab 1.1- Setting Up for Success

In this lab exercise, we cover how to set up your system so that you can work through the various lab exercises we have provided. If you have any issues with the setup, please ask the instructor or TA for assistance so that you will be able to complete the exercises throughout the rest of the course.

Social Engineering Goals

In the next section, we're going to dive into some of the major goals of a pen test that includes social engineering.

Test Categories

- Physical social engineering
  - Tailgating
  - On-site document/asset theft
  - Physical security testing
  - Media drops (on-site)
- Non-physical social engineering
  - Phishing
  - Pretexting
  - Media drops (post-drop)

Before we get to the major goals of the social engineering test, let's talk briefly about the major categories of social engineering. We'll be spending some time in class covering most (not all) on this list. The first type of social engineering engagement is on-site, or physical social engineering. These types of engagements may involve the following activities:

- **Tailgating**: Tailgating is a simple concept—you try to illicitly gain entry into facilities by following others in or just circumventing physical access controls.
- **On-site document/asset theft**: During some on-site social engineering engagements, targets will be interested in whether you can gain access to sensitive documents and data (papers, hard drives, and other media) and leave the facilities. In essence, this is simple theft by a malicious party.
- **Physical security testing**: Additional types of physical security testing may include bypassing cameras or security guards, lock picking and bypassing other physical access controls like fences, doors, and others.
- **Media drops (on-site)**: If media drops are included in the scope of the engagement, the media (usually USBs) will need to be dropped at various locations on-site.

Non-physical social engineering types include the following:

- **Phishing**: Phishing involves sending malicious e-mails to entice users into clicking links or opening malicious attachments.
- **Pretexting**: Pretexting involves calling targets on the phone and attempting to convince them to perform some action advantageous to the attackers.
- **Media drops (post-drop)**: If media drops were performed on-site, the follow-up activities may include logging clicks from users or following up with full-blown pivoting through the environment after endpoint compromise.

SE Goal: User Awareness Assessment

- The most common social engineering goal for target organizations is security awareness validation
- This is commonly tested through phishing and pretexting engagements:
  - Will users click on links or open attachments?
  - Will users give away sensitive information over the phone?
  - Will users report the suspicious e-mail or call?

The most common type of goal for social engineering engagements is validation or refutation of the target organization's security awareness training program. Most organizations today have some sort of security awareness program in place and often emphasize phishing e-mails and suspicious behaviors, such as unsolicited phone calls and people trying to gain access to buildings and facilities without authorization. While challenging people on-site without a badge is often taught during security awareness training, the most emphasis in training is usually placed on phishing and pretexting.

Social engineers are often called upon to test and validate this training by sending malicious e-mails or placing phone calls to users and help desk teams to try and have them perform password resets or give up sensitive information.

SE Goal: Data Exfiltration

- Another common goal of many social engineering engagements is data exfiltration
- Can social engineers:
  - Access sensitive data?
  - Get the data out of the physical premises?
  - Demonstrate exfiltration methods that are not detected by security teams?

Exfiltrating data from a target organization is also a common goal of social engineering engagements. During the course of many social engineering activities (phishing or USB drops that lead to system compromise, for example), testers may discover sensitive data of various types. Sometimes this data will be discussed beforehand as a focal area of the engagement (for instance, companies that process payment card data may want to emphasize or focus on the discovery of plaintext payment card information), but often the data discovered will be somewhat ad hoc, leading to discussions with target personnel throughout the engagement. Common data testers may uncover includes personnel files and data, financial data, business plans and other sensitive internal data, medical information and more.

As part of the goals of data exfiltration, testers may be tasked with accessing sensitive data and then trying to get it out of the facility or logical network. In some cases, particular exfiltration methods or specifics will be requested, such as DNS or ICMP tunneling, encrypted formats, unusual HTTP headers, USB drives, and more.

SE Goal: Exploit Execution

- In many pen tests, targets will be interested only in "click counts" or other basic metrics related to security awareness
- In other tests, however, one of the primary goals will be exploit execution:
  - Through phishing (browsers/attachments)
  - Through media drops (malicious files and autorun)
  - Through purposeful implants

During some social engineering projects, you will likely find opportunities to attempt exploit execution. This will most often happen when performing phishing and media drop tests but may also be allowed with purposeful implants to machines during on-site visits (usually via rebooting to USB drives). Whether this type of testing is allowed will usually depend on whether it's a full-blown pen test or red team test versus just a simple social engineering exercise to validate security awareness.

SE Goal: Configuration/Patch Testing

- Testing specific system configurations during social engineering tests can also be a valid goal
- Usually, pen tester goals include:
  - Confirming whether hardening has been applied to a system
  - Confirming patch status for systems
  - Confirming default or easily compromised settings

Sometimes during social engineering tests, testers will be asked to validate the settings on particular servers or workstations. Most often this will be a secondary goal after compromise or access to systems is achieved (usually the primary goal, or one of them).

In these cases, testers are usually looking for specific indicators specified by the target organization. These often include hardening configuration items that have been ignored or missed during system builds, a lack of patches applied to the systems, or the presence of default or simple configuration settings that could also easily lead to compromise.

SE Goal: Physical Security

- Testing physical security is a common SE goal
  - Sometimes more in line with “red team” tests
- Pen testers may assess:
  - Security guard attentiveness/effectiveness
  - Locks/doors
  - Logical/electronic access controls
  - Camera placement/visibility
  - Staff attentiveness

The final major goal for many social engineering tests is to validate or test physical security at target sites. Doing physical testing starts to veer into more “red team” types of tests that may include bypassing guards, picking locks and avoiding cameras and other controls.

Some of the most common goals for physical security assessments include:

- **Security guard attentiveness/effectiveness**: This is, in fact, part of tailgating activities fairly often, but may be a focused effort or goal as well.
- **Locks/doors**: While lock picking and door/window/gate bypass are more physical hacking than simply social engineering, it is sometimes coupled with social engineering efforts.
- **Logical/electronic access controls**: This involves attempting to bypass badge readers, biometric access controls, and motion detectors.
- **Camera placement/visibility**: Trying to avoid cameras, as with security guard bypass, is somewhat expected when tailgating on-site. Though this may also be a particular goal of the engagement as well.
- **Staff attentiveness**: Do employees working in a facility challenge visitors without badges? Assessing this is often a secondary goal of on-site tailgating activities as well.

Social Engineering: Where to Focus

- In conclusion, make sure you understand the goals and requirements of the target organization
- Different organizations and teams will be focused on:
  - Pen testing
  - Security awareness training
  - Risk analysis

To wrap up the planning discussion, let's summarize. The target organization will likely have specific goals in mind for the social engineering activities that are part of the pen test, but it's helpful to have a conversation up front to determine where the efforts should be focused—always keep the endgame in mind!

Some organizations are focused on more red team activities, which is really pen testing with some social engineering thrown in to accomplish the goals of the test. In other words, social engineering is usually a means to an end in those projects. If the goal of the target organization is to measure and tune security-awareness training programs, then social engineering may be the primary aspect of testing. If the organization is looking at the "big picture" of risk, then there may be some specific aspects of testing that include physical testing, exploit execution and who knows what else. Have a conversation when planning the scope and engagement specifics, and then plan from there!

Now that we've got planning the engagement out of the way, let's get down to brass tacks. We need to start determining what our targets are and perform reconnaissance on them.

In some types of tests, the target organization will provide all the details on targets—e-mail addresses, phone numbers, pretext context, types of phishing templates to use and so on. In many cases, however, social engineering tests will include only basic information to start off with, or perhaps none at all. A more "black box" approach to social engineering will include the discovery of targets and learning enough about them to perform targeted attacks when needed. This next section focuses on targeting and reconnaissance activities that will enable you to perform advanced social engineering activities.

Information Gathering Phase

- Unearth initial information about target(s)
- Locate network ranges (if applicable)
- Discover services/access points of entry
- Perform reconnaissance on employees and related people
- Look for information that could be useful in exploiting people and targets

After the Determine the Scope phase has been successfully completed with a contract or plan to get underway with the test, it is time to go to the Information Gathering phase of penetration testing. At this phase, it is critical to think like an attacker in the Reconnaissance phase. What types of information would an attacker be able to obtain and consider useful? Once the information is identified, what are the sources of the target information? What methods can be used to easily obtain the information from the sources in a way not to be easily detected? There are several types in the Information Gathering stage of penetration testing. These steps are applicable to determining the types of network capabilities of the target system. We explore each of the following steps in detail in later slides:

- Unearth initial information about target(s)
- Locate network ranges (if applicable)
- Discover services/access points of entry
- Perform reconnaissance on employees and related people
- Look for information that could be useful in exploiting people and targets

Information Types of Interest

- Types of information:
  - Address ranges (if applicable)
  - E-mail addresses
  - Contact information
  - Devices and applications used
  - Public systems/data
  - Company/organizational information
  - "Mistakes" (data exposed inadvertently)

Information is a key resource to any organization, and those who have access to sensitive corporate knowledge are in an extremely powerful position to compromise the system. During the Determine the Scope phase, the tester will ascertain several key organizational assets, their role in supporting the organizational mission, and the individuals who have control over those assets. The identified assets will store, process and transmit important information from a testing perspective that will become useful in future phases of the testing. In the Information Gathering phase, the tester will look to acquire non-intrusive information about the targets and employees. There are several sources to acquire the information above, which will be discussed on the next slide.

One of the critical pieces of information from a networking perspective is the network address ranges that may be a factor in other pen testing activities. System administrator e-mail address, organizational contact information, types of network devices and applications used will also be useful for various types of activities. This Information Gathering step in the process is typically called footprinting. The collected information will enable the tester to strategically focus their resources to build a map of the organization's social infrastructure. By having this information, the tester will be able to use additional networking and social engineering techniques and choose the approach that best fits the solution to exploit multiple vulnerabilities in the target organization. In addition, collecting all available information will enable the tester to ensure that information which would be critical to a successful penetration test is not overlooked.

Traditional Sources for Recon

- Search engines: Google, Bing, Baidu
- SHODAN
- DNS/WHOIS
- Open source/public info sites
- Social media sites
- Job sites

There are many traditional sources of reconnaissance. Search engines can definitely go a long way toward helping testers uncover data about targets, which we cover in more detail in a moment.

We also have sites like SHODAN, which is a specialized search engine for locating vulnerable systems and applications. DNS and WHOIS queries can help to locate infrastructure information, as well as potential target personnel and contact information.

Open source and public information sites can provide details about a target's employees, as can the target's own website. Job sites may reveal information about potential technology targets that are useful throughout the pen test.

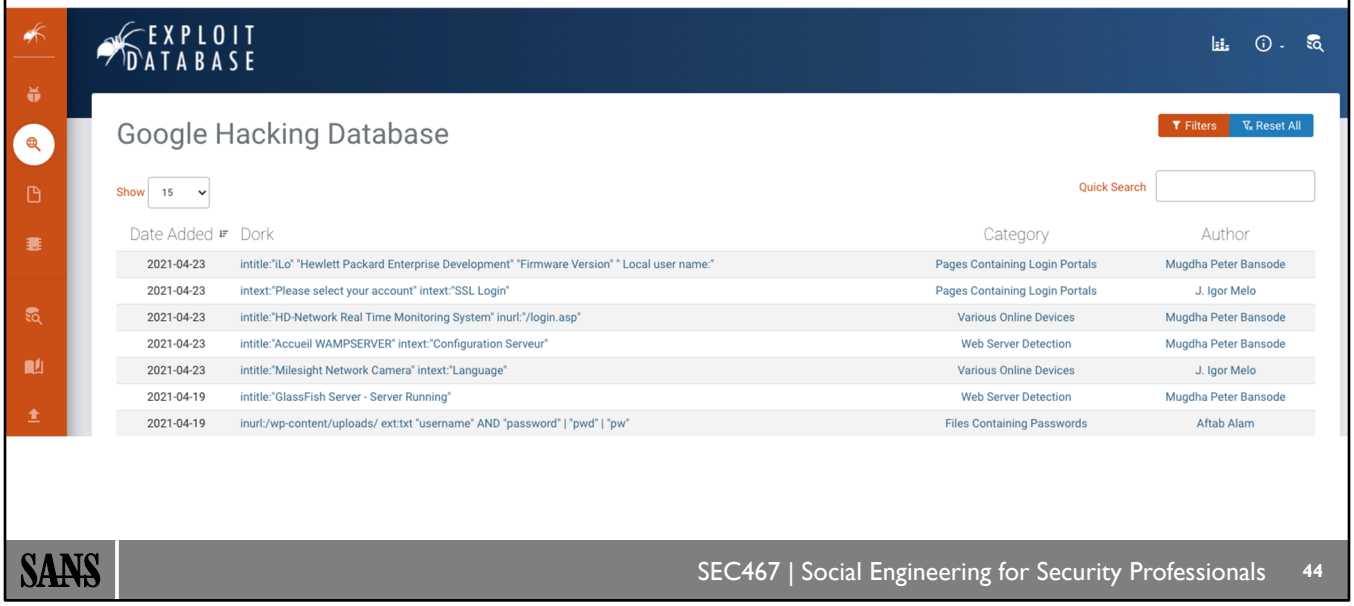
For targeting people in particular, social media sites can be useful too. We take a closer look at all of these in the next section.

Using Search Engines for Recon

- Google is your friend:
  - Use “site:”
  - Work with URLs to construct faster and smarter queries
  - You can use “filetype:” if you are searching for intellectual property leakage
  - Exclude common file types with “-ext:”
  - Try “intitle:” if you are hunting a specific setting
- https://www.exploit-db.com/google-hacking-database

You can find all kinds of information about a target by using Google or any other favorite search engine. The book *Google Hacking for Penetration Testers* by Johnny Long provides a lot of tips for streamlining your searches. There are often news articles, whitepapers and other documents that reveal potentially secret information about a target.

Google Hacking Database



A 'Google Hacking Database' lists helpful Google search strings that can be used to collect additional information about the target. Leveraging Google or other query systems, such as Yahoo, has several benefits, to include reduced time for the tester to exploit specific services or ports on the target and to quickly acquire information such as default application passwords or specific application vulnerabilities for use in exploitation or social engineering activities. This database is now found at https://www.exploit-db.com/google-hacking-database

Google Hacking (1)

- Using "site:" to find interesting hostnames:
  - First, hone it down. "-site:" is a negative operator. It strips out the site you specify.
  - site:cisco.com -site:www.cisco.com results in 241,000 hits (lots of unique host names in the FQDN)
  - site:cisco.com -site:www.cisco.com – site:tools.cisco.com results in 188,000 hits (still lots of unique host names in the FQDN)
  - site:cisco.com -site:www.cisco.com -site:tools.cisco.com -site:newsroom.cisco.com –site:forums.cisco.com -site:blogs.cisco.com results in 88,500 hits. This can be repeated for some time.

This slide describes how you can use the site: operator to find interesting hostnames and to reduce your results significantly with the "-" operator.

Google Hacking (2)

- Getting more specific:
  - Exclude file types with a negative query
  - ext means filetype
  - site:fbi.gov returns 124,000 hits—way too many hits!
  - site:fbi.gov -ext:htm -ext:html results in 9,340 hits

Using negative operators such as "-ext:" can help to reduce results again, getting you closer to what you're looking for. "-ext" will remove pages and information from Google queries with specific extensions.

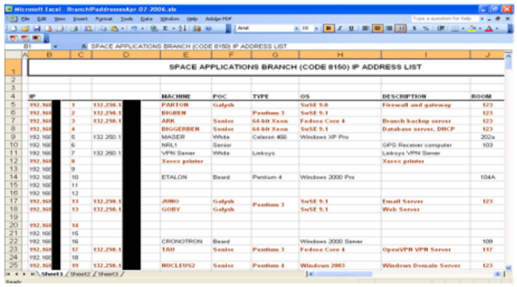
More Info on Filetype

- Check https://filext.com/—Google can find all of these
- Try them all—you will be amazed at what you find
- Example: filetype:rdp rdp
- A number of filetypes out there contain usernames and passwords, shell command histories, logged data of all sorts, configuration details etc.
- Try a search on “bash_history” in an index listing

Google can help you track down a lot of different document types, many of which are found at filext.com. You can use your imagination here when querying Google for different file types and data in a target organization.

Google Hacking (3)

- Examples:
  - site:.mil intitle:index.of /admin



  - filetype:ini inurl:ws_ftp

Let's look at some examples of things one can find while searching Google.

site:.mil intitle:index.of /admin leads to a spreadsheet shown in the slide, with system names and addresses, etc.

filetype:ini inurl:ws_ftp leads to FTP configuration files with usernames, passwords and more!

Search Engine Queries for SE (1)

- Start with the simple things:
  - E-mail addresses for the target: “@targetorg.com”
  - Start with a person’s name: “Bob TargetOrg”
  - Also add the company name/site: “Bob TargetOrg” targetorg.com
- You can also pair people’s names with filetype searches to find files associated with individuals

When you start using search engines for social engineering, you can start with simple queries that include people’s names, as well as names and the target organization name and/or site paired together. A more general sweep for e-mail addresses associated with the target organization can be performed with the “@targetorg.com." This is not the most efficient way to find e-mail addresses—better tools are available, and we cover those shortly. However, this is a solid start, and you can easily move on from this to more advanced queries.

Combining different searches with names will often locate interesting information too. For example, combining filetype searches with names will sometimes turn up files authored by people you’re targeting, and you may be able to use metadata extraction tools such as FOCA and ExifTool to determine the technology they’re using. This, of course, comes in handy for client-side exploit attempt.

Search Engine Queries for SE (2)

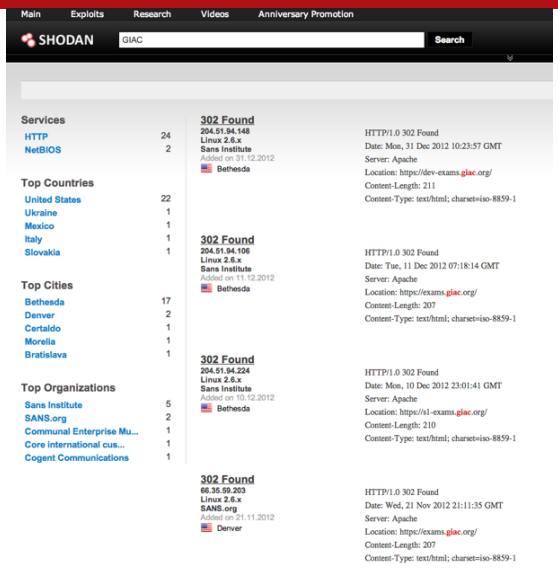
- In addition to the GHDB queries and query categories, some general queries that are most useful include:
  - login | logon
  - username | userid | employee.ID | “your username is”
  - password | passcode | “your password is”
  - admin | administrator
  - intranet | help.desk

In addition to the techniques already covered, some other interesting queries specifically for social engineering include the following:

- **login | logon**: Looks for login pages within the target site.
- **username | userid | employee.ID | “your username is”**: Looks for potential credential information about target users within the target organization.
- **password | passcode | “your password is”**: Can help find credentials (rare) and more often discovers pages that help users recover passwords if they have lost or forgotten them.
- **admin | administrator**: Can locate error pages, information about admin apps and pages, admin login pages and more.
- **intranet | help.desk**: This query can help to locate contact information for a help desk (useful for phishing and pretexting exercises), as well as login portals for intranet applications and services (which may offer useful or interesting hints for later targeting, if nothing else).

SHODAN for Recon

- Search engine at www.shodanhq.com
- Lots of simple filters you can use:
  - **net**
  - **city**
  - **country**
  - **port**
  - **before**
  - **after**
  - **os**



Shodan is essentially a search engine for vulnerable systems and apps. With your search queries, you can include filters to get more specific like the following:

- **net**: netblock specification
- **city**: City of system/target location
- **country**: Country of system/target location
- **port**: Service/app ports
- **before**: Posted before a certain data
- **after**: posted after a certain date
- **os**: OS identified in use

Shodan may have some applicability to social engineering, especially if you are targeting people who work in technology or have administrative control over online technology that Shodan can uncover.

DNS and WHOIS

- WHOIS lookups provide us with IP blocks and name servers
  - Contact info is sometimes useful for SE
- DNS information from name servers can provide a lot of information:
  - NS: Nameserver records
  - A: Address records
  - MX: Mail Exchange records
  - PTR: Pointers, inverse lookup records
- Micah Hoffman has a great blog post that uses the ViewDNS.info site to gather info with DNS: https://webbreacher.com/2016/08/09/harvesting-whois-data-for-osint/

A `whois` query provides information on the target, the registered domain name, registered name servers, IP addresses and contact information. There are several different `whois` websites and desktop clients, such as Sam Spade, for obtaining `whois` information. Some of these services may reveal more information than the others, so it is best to use several different methods of `whois` lookup. You can also use whois from the command line on many operating systems.

Domain name lookups can help us build on our recon efforts from WHOIS. We now have some domain name info and name servers, and we can start to query them for other record types. The main types we are interested in include:

- **NS**: Nameserver records
- **A**: Address records
- **MX**: Mail Exchange records
- **CNAME**: Canonical Name records
- **SOA**: Start of Authority records
- **PTR**: Pointers, inverse lookup records

Open Source and Public Info Sites

- There are many additional sites that can offer information about target organizations and users:
  - EDGAR: If the target company is publicly traded, organization info will be available here
  - Hoovers: A paid site that sells reports on companies
  - State and government sites: Various government sites may offer information too

Sometimes government sites can offer some good information on targets and people as well (especially company officers and other high-profile targets). Some of these types of sites include:

- **EDGAR**: If the target company is a publicly traded, organization info will be available here. EDGAR is a search feature of the U.S. Securities and Exchange Commission (SEC) and can be found at https://www.sec.gov/edgar/searchedgar/webusers.htm.
- **Hoovers**: A paid site that sells reports on companies, similar to EDGAR but with more options. A free subscription is available but searching here over time will require a subscription (you can also pay for one or more reports individually). Available at http://www.hoovers.com/.
- **State and government site**s: Various government sites may offer information too, especially at a local level (news stories about businesses in the local community, recent activity etc.).

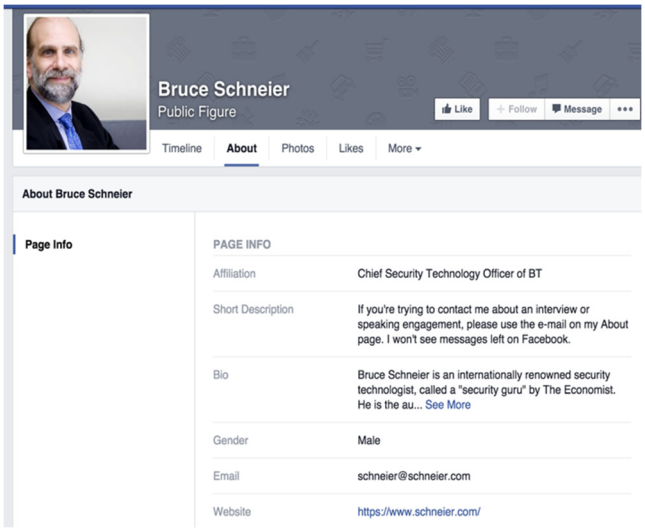
Social Media Recon

- Social media has become one of the most fruitful sources of social engineering info
- Many targets post entirely too much information about themselves:
  - Location
  - Employment
  - Contact info
  - Hobbies and interests
  - Family information

Social media sites and applications can provide social engineers with enormous amounts of useful data when targeting specific people and companies. Many companies have their own social media accounts where they post information about the company, events that are happening, news and even pictures and information about employees. The employees may very well have their own sites and information as well.

Facebook

- Facebook can often provide a lot of personal information:
  - Friends
  - Hobbies
  - Photos
  - Recent activity
  - Location
  - Employment



Facebook can often provide a lot of personal information about targets and target organizations. Examples of the most common and prevalent data types include:

- Friends
- Hobbies
- Photos
- Recent activity
- Location
- Employment

For obvious reasons, this information is highly useful to social engineers! We can craft much more plausible phishing e-mails, pretexting arguments and attack strategies overall with the amount of information many post in their Facebook profiles.

Facebook is found at http://www.facebook.com.

Twitter

- Twitter can tell you a lot about a person:
  - Where they have been recently
  - Who they are friends with
  - Hobbies and interests
  - Location
  - What they had for lunch ☺

Twitter is a simpler, higher volume interaction tool for many individuals, especially those in the tech industry. Many companies also have Twitter profiles. Twitter public profiles can tell you much about a person's recent activity (or lack thereof). Many people list their hobbies in their profiles and as their industry and other stats. Many people also tweet pictures of food and other silliness, but you can learn from this. If you want to "accidentally" meet someone or try and shoulder surf their activity, find out where they have coffee or eat out.

Twitter can be found at http://twitter.com.

LinkedIn

- LinkedIn has more "professional" information about people and companies

LinkedIn is a site that most people use for posting professional information and updates, so you're unlikely to see a picture of someone's lunch here unless she's a chef. However, companies and individuals post ridiculous quantities of information here for prospective social engineers to collect.

LinkedIn can be found at http://www.linkedin.com.

Other Social Media Sites

- There are many other social media sites that may be fruitful for social engineers:
  - Google+
  - YouTube
  - Flickr
  - Instagram
  - Pinterest
  - Blogger.com
  - TikTok

There are an enormous number or social media sites online today, not all of which will be useful during the course of social engineering engagements. The best approach is to scour the most common ones out there and if something you find leads you to another site, it may be worthwhile to look into whether the information there is useful. However, perusing social media sites can take a lot of time and may not really prove useful after the first few sites are exhausted.

Several other sites of interest may include:

- **Google+**: Profile information, blog posts, connections, and "hangouts"
- **YouTube**: Videos posted by targets
- **Flickr**: Pictures posted by targets
- **Instagram**: Pictures posted by targets
- **Pinterest**: Ideas, crafts, recipes and general sharing site for anything
- **Blogger.com**: Blog posts written by targets
- **TikTok**: Short videos posted by targets

Job Sites

- Job sites can often reveal information about technology in use at target organizations
  - Individual social engineering targeting is usually not the goal
- Finding out what technology is in use can help with phishing and media drop exploitation and payload execution
- Common sites include Monster.com, Indeed.com, GlassDoor.com, and CareerBuilder.com

Job sites often give away juicy tidbits of information about technical positions that are open and will usually provide clues about the technology in use at the target organization.

In particular, the most valuable information for social engineering includes the list of desktop technology in use, as this can be leveraged for creating exploits and payloads that will be run during phishing campaigns or through media drops on-site. If the target is running certain versions of Windows, Java, Adobe Reader and various browsers, many times more successful exploits can be crafted. The same holds true for antivirus and host-based security tools—if you know the target runs Symantec Endpoint Protection or Carbon Black Bit9, you may have to come up with workarounds for payload execution.

Common job sites in use include Monster.com, Indeed.com, GlassDoor.com, and CareerBuilder.com, although there are many, many more.

The Harvester

- The Harvester is a fantastic recon tool that can search Google, LinkedIn, Bing, Shodan and more for:
  - DNS info
  - People
  - E-mails
  - Services known to the site/domain

The Harvester is a reconnaissance tool written by Christian Martorella that looks for information related to sites and organizations. The Harvester can query Google, Bing, Shodan, PGP key servers and LinkedIn to discover an amazing amount of useful data for social engineers. The information you can find with the Harvester includes e-mails, target names, services associated with the domain or sites and more.

The Harvester is built into Kali but can also be downloaded from https://code.google.com/p/theharvester/.

Metagoofil

- Metagoofil is a full-featured search engine scraping tool that can use Google to pull down files with a flexible syntax and approach
- Options:
  - -d <site>
  - -t <filetypes>
  - -n <quantity of docs to download>
  - -l <number of results>
  - -o <output directory>
  - -f <report file>

Also finds:
- Users
- Software
- Paths
- Servers

Metagoofil, also by Christian Martorella, is a powerful tool that allows you to query a site on Google and look for files and any metadata within those files, as well as other useful information such as e-mail addresses of users associated with documents discovered.

Basic options are simple:

Options:

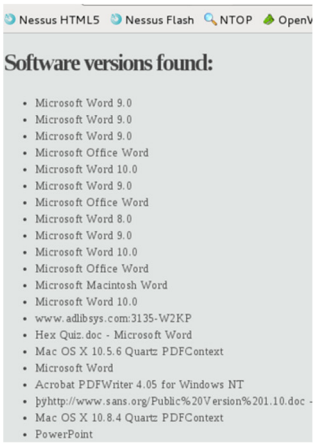
-d <site>
-t <filetypes>
-n <quantity of docs to download>
-l <number of results>
-o <output directory>
-f <report file>

An example of a site search on sans.org for 100 results with up to 20 documents of types doc and pdf would look like this (output to a folder named "sans" with a report):

```
metagoofil -d sans.org -t doc,pdf -l 100 -n 20 -o sans -f results.html
```

Metagoofil Example

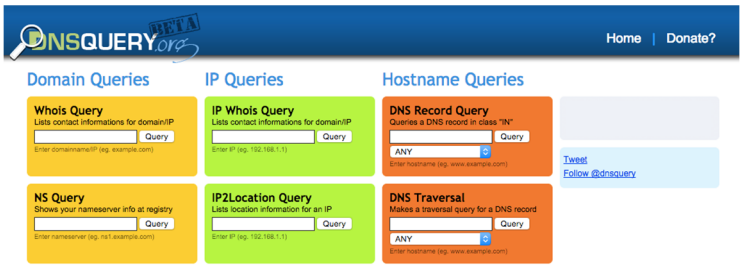
```
root@kali: /tmp/SE                    root@kali: /tmp/SE
root@kali:/tmp/SE# metagoofil -d sans.org -t doc,pdf -l 100 -n 20 -o sans -f results.html


*********************************************************
*     /\/\   ___| |_ __ _  __ _  ___   ___  / _(_) | *
*    /    \ / _ \ __/ _` |/ _` |/ _ \ / _ \| |_| | | *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | | *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_| *
*                         |___/                       *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*********************************************************

[-] Starting online search...

[-] Searching for doc files, with a limit of 100
        Searching 100 results...
Results: 33 files found
Starting to download 20 of them:
----------------------------------------
```



This slide depicts some of the data gathered during a simple query against the sans.org domain, looking for DOC and PDF files. Not only did we find many interesting documents (mostly written by SANS students), but we culled people's names, e-mail addresses, software versions, and even local directory paths associated with SANS by executing this query—all in just seconds!

DNSquery

- DNSquery is a simple network recon tool online at https://dnsquery.org/
- You can do a number of DNS and HTTP queries of any site, as well as pings and traceroute
- This can be a useful tool for basic network intelligence

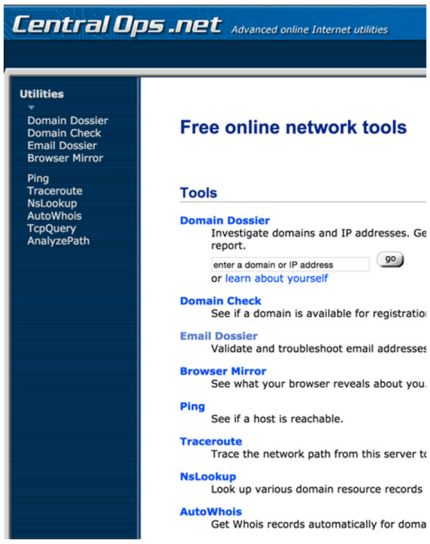


DNSquery is not an in-depth tool but can do simple and basic network recon for sites and services online. The site is found at https://dnsquery.org and it can be used to query DNS, perform pings and traceroutes, and perform HTTP queries against sites.

Why would social engineers need a site like this? Simple—it's anonymous! If you want to perform a basic DNS query for a target site, doing it via DNSquery may prevent you from showing up in log files.

CentralOps

- CentralOps is another online recon tool but can do more than just network recon
- CentralOps can query and validate:
  - E-mail addresses
  - Domain information
  - Browser info
  - DNS
  - Traceroute

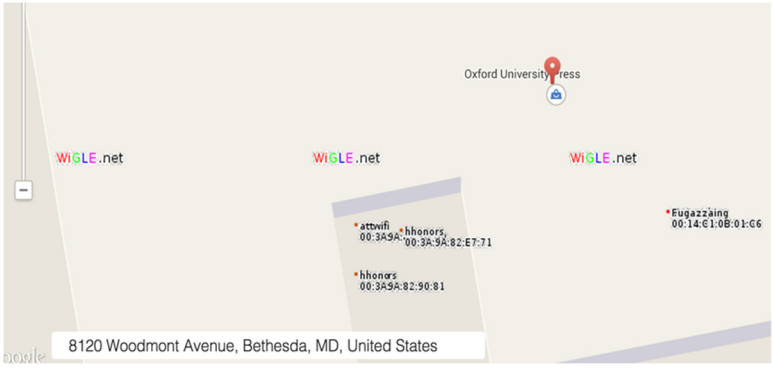


CentralOps.net is a site that can also perform network-focused recon activities but can also do e-mail validation, DNS queries, browser checks and graphing of traceroute data.

The most useful information from CentralOps for social engineers is likely the e-mail validation function, but the site can also be useful for DNS queries and more.

Wigle.net

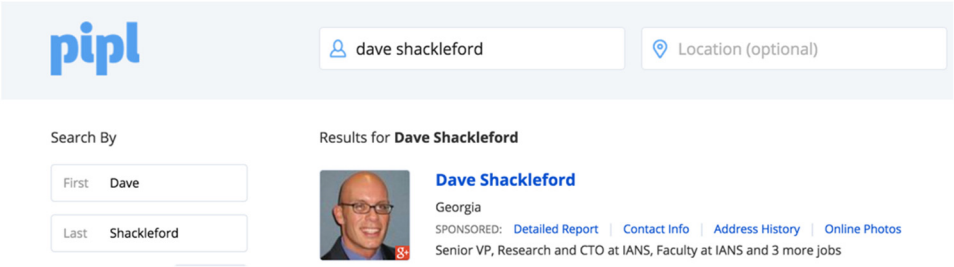
- Wigle.net can show you wireless networks observed around addresses you query
- This can be very helpful for on-site work later in your social engineering engagements



Wigle.net is a simple site that allows you to enter a physical address and look for known wireless signals seen around the area. If you plan to perform on-site activities, this is likely useful information for potentially luring users into connecting to illicit access points or trying to hijack wireless users.

Pipl

- Pipl.com is a great start to targeting people
- In one query, Pipl will look up information about a user's jobs, locations, education and more
- Today, Pipl has a number of sponsors that can provide more detail for a fee



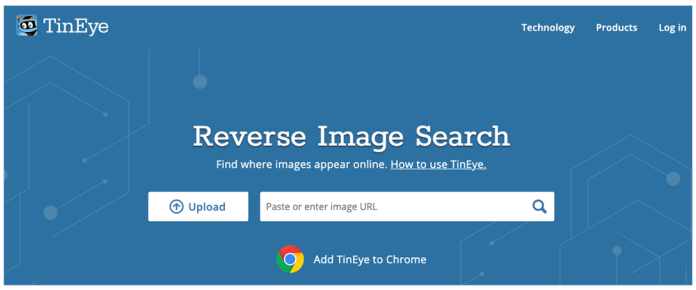
Pipl.com is a site that can help you get started in tracking down user information. While most of the data in Pipl results is "sponsored" (code for "pay for it"), there is still a fair amount of basic data about users that may get you started in performing recon and general searches.

The most valuable data routinely provided by Pipl includes names, education, geographic locations and affiliated groups and organizations.

Today, Pipl is primarily a paid service, but trial accounts are available.

TinEye

- TinEye is a unique service that does a reverse lookup on images
- This can help social engineers determine if images from a user's blog or site come from somewhere else, which becomes fodder for social engineering!



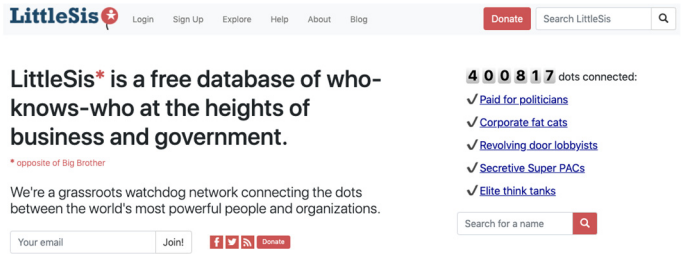
TinEye gives you a unique capability to perform "reverse queries" on images you upload. What can social engineers glean from this kind of information? How can this be useful?

Answer: MANY ways. Here are some examples:

- Social engineers could take images from a user's blog or personal site and find out where they are posted currently
- Images affiliated with a user or organization may have come from somewhere originally or have a strong affiliation with sites that warrant additional recon
- Affiliated sites and organizations may be useful for creating pretexts and phishing campaigns specifically targeting users

LittleSis

- LittleSis lists the rich and powerful (or top influencers) with their relationships and other valuable information
  - Sign-up is required but is free
- LittleSis allows you to search for people in your target org, finding:
  - Relationships
  - Similar people
  - Giving and donations
  - Political affiliations
  - Additional data
- Site at https://littlesis.org

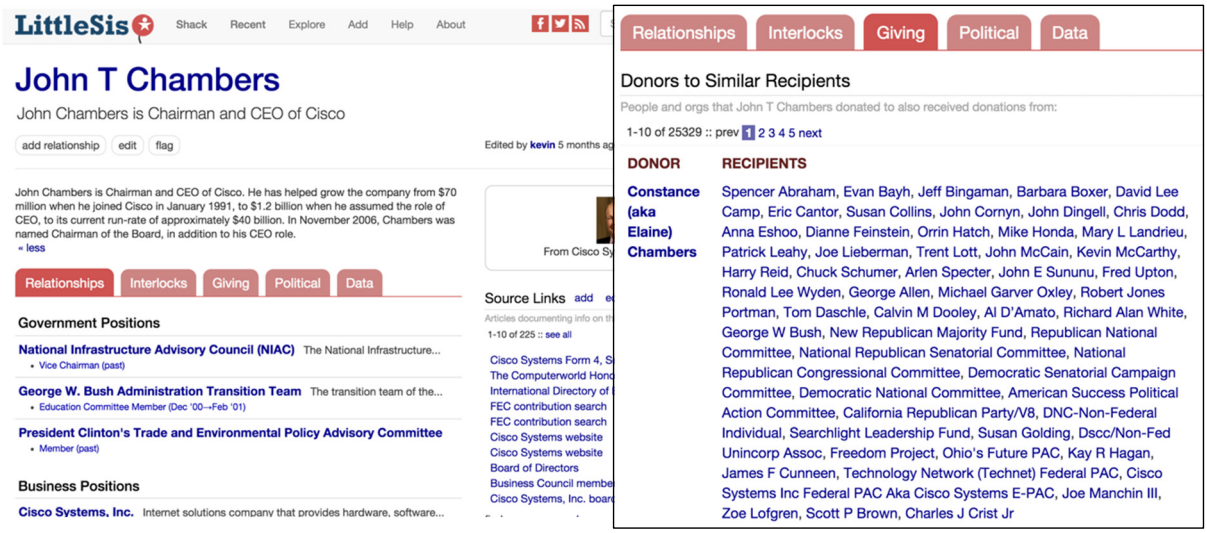


LittleSis allows you to search for people in your target organization, finding:

- Relationships
- Similar people
- Giving and donations
- Political affiliations
- Additional data

LittleSis requires a free account to use and tends to target more high-profile people like top executives. If you are tasked with social engineering people at this level, LittleSis will quickly become an invaluable resource.

LittleSis Example

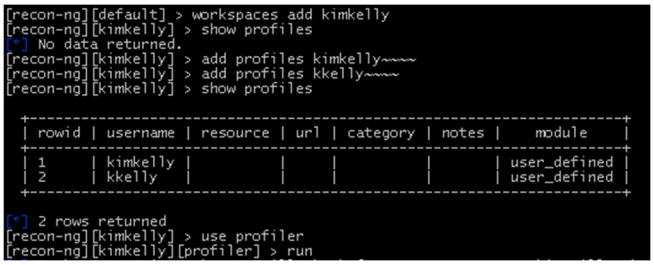


This shows a simple LittleSis query for John Chambers, the CEO of Cisco (his picture is blocked in the screenshot). LittleSis lists his known affiliations, political leanings, politicians and their causes supported and more.

In this example, we can also dig into the donations made by Mr. Chambers (or his wife, more likely). These could very easily become pretexts for social engineering if we were hired to target Mr. Chambers during a pen test.

Recon-NG

- Recon-NG is one of the most flexible frameworks available for performing recon activities today
- Numerous recon modules are available (66 currently) that can look up people, companies and more
- The framework is intended to emulate the command line operation of Metasploit
- A fantastic recon module for profiling people is Micah Hoffman's "Profiler" module
- May not be updated often, but still useful today



Recon-NG is one of the most versatile frameworks for performing recon activities available today. The framework was built by Tim Tomes, who developed the tool to emulate the same interactive model found in Metasploit. The framework can be downloaded at https://github.com/lanmaster53/recon-ng.

Recon-NG has a number of recon modules available, including domain lookups, social media targeting, geolocation information and many more. Micah Hoffman's "Profiler" module is a fantastic tool for looking up user information online, and he describes it in detail on his site:

https://webbreacher.com/2014/12/11/recon-ng-profiler-module/

Hybrid Tools

- These tools go beyond “simple” recon
- These tools can also:
  - Build relationships
  - Extract metadata
  - Extract location data
- Tools include:
  - Maltego
  - FOCA
  - ExifTool
  - Cree.py

While many recon tools and sites are specific to one data type or purpose, there are several additional tools that you should know about that go further than this. Some of these “hybrid” tools can help you to build out relationships and more complete target profiles, which we’ll cover in a moment. Examples of these tools include Maltego, which can help you build highly developed target profiles, and FOCA, which is useful for extracting metadata from files and sources. ExifTool is another excellent utility for extracting metadata from files.

Cree.py is a tool that allows pen testers to extract location data from tweets and photos, similar to PushPin (part of Recon-NG) in some ways.

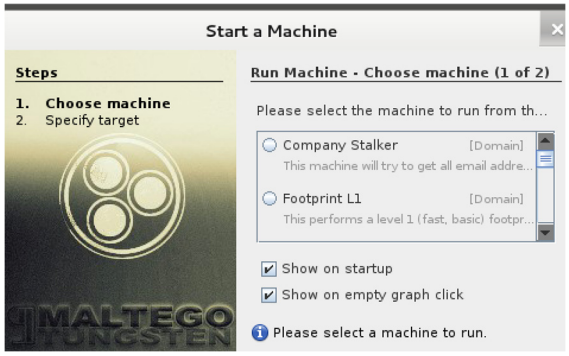
Maltego

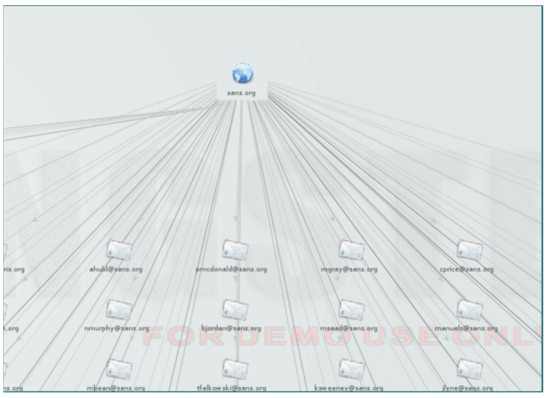
- Maltego may be the ultimate profiling tool available today
- Offered in two editions: Community and Licensed
- The community edition is free, and offers some basic functionality and query models
- Maltego also has several pricing models available
  - Professional edition is currently $999/year
  - Enterprise's edition requires a quote
- Can perform "transforms" of one data type to another

Maltego is a tool that can be used to perform a wide variety of recon activities. With Maltego, you can look up a company, person, domain, or additional data types, and Maltego's servers will scrape a huge data set of publicly available data to find information about your targets. Once the initial data has been retrieved, Maltego will build a map of the target data and then the fun really begins.

Maltego allows you to perform "transforms"—you can turn any one data type into another by asking Maltego to go out and fetch it. For instance, you can ask Maltego to find PGP keys seen with e-mail addresses or phone numbers seen with usernames.

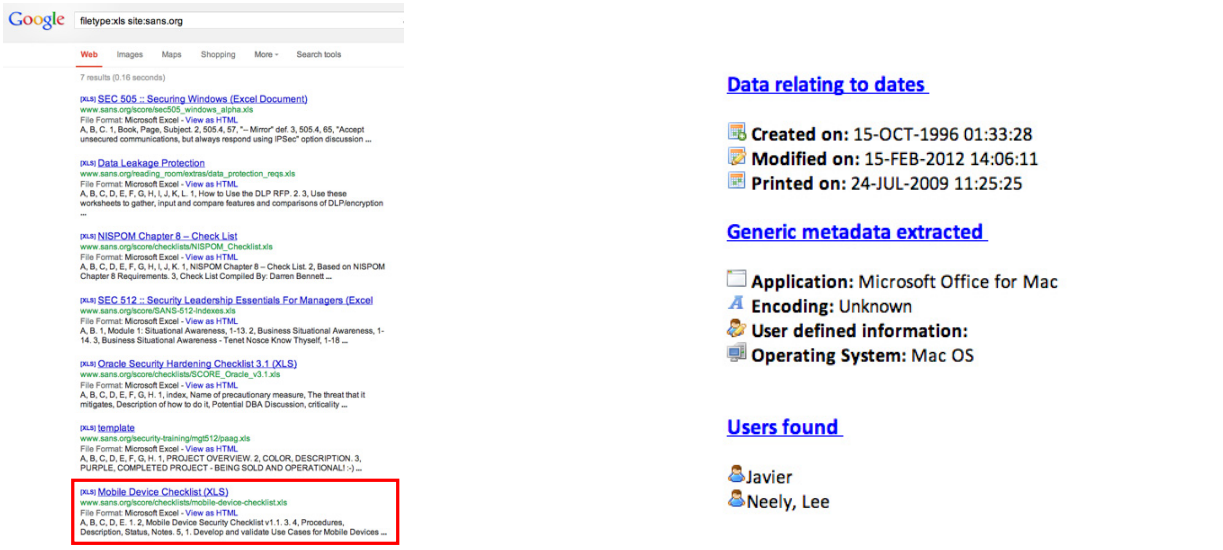
Maltego: SANS Stalking





In this screenshot, we used the Maltego Community edition to "stalk" SANS and find e-mail addresses and other employee information. In just about a minute, we had hundreds of pieces of information to use in targeting operations.

FOCA



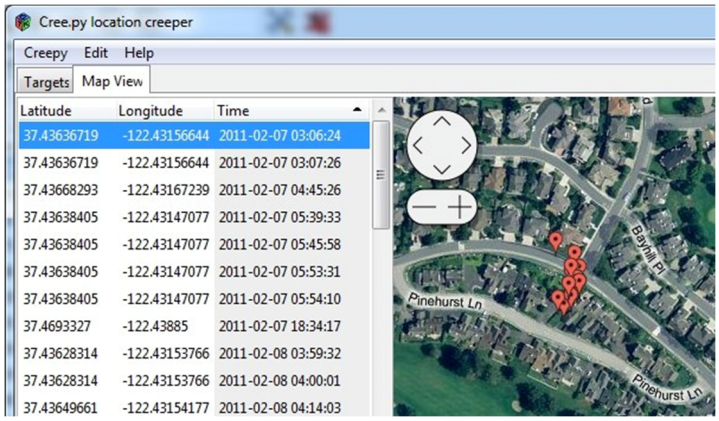
Metadata is another area of interest for recon. There's a LOT of data embedded in common file formats, often without people realizing it at all. Office docs, pictures etc. are all chock full of data that attackers and pen testers can look for during the recon phase.

FOCA is a tool available from https://github.com/ElevenPaths/FOCA. Although the tool is not currently being updated, it is still useful for performing some types of queries.

FOCA can pull enormous amounts of data out of files as well, including the same things described with ExifTool and even more! Another great tool to routinely run against documents and other posted data.

Cree.py

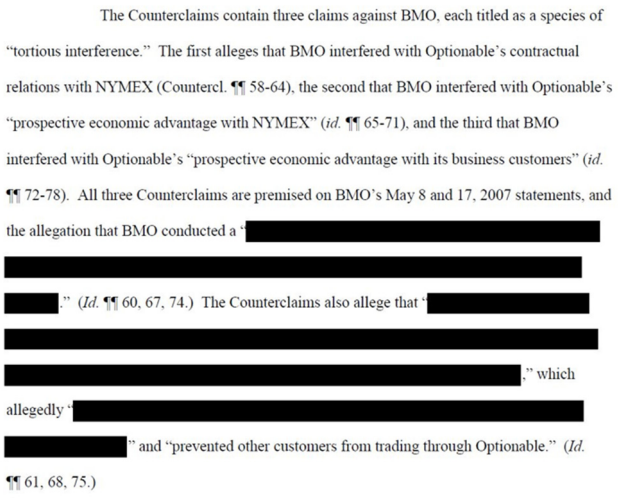
- Cree.py is a geolocation mapper for social media sites including Twitter, Flickr, Google+ and Instagram
- Profiling targets is very simple to do with the built-in wizard



Cree.py is a program that allows social engineers to track geolocation of their targets based on social media posting. The tool is available for Windows, Linux, and Mac operating systems at http://www.geocreepy.com/, and has a number of modules including Google+, Twitter, Instagram, and Flickr. These social media sites require an API key or account access to use properly, but social engineers will find much to love if they need to track target movements and site visits in a particular region or location.

Redacted Documents

- If you find documents that have redacted content, see if the content is REALLY redacted/removed
  - Sometimes, it's just an overlay and you can highlight content and even copy it out!



The Counterclaims contain three claims against BMO, each titled as a species of "tortious interference." The first alleges that BMO interfered with Optionable's contractual relations with NYMEX (Countercl. ¶¶ 58-64), the second that BMO interfered with Optionable's "prospective economic advantage with NYMEX" (*id.* ¶¶ 65-71), and the third that BMO interfered with Optionable's "prospective economic advantage with its business customers" (*id.* ¶¶ 72-78). All three Counterclaims are premised on BMO's May 8 and 17, 2007 statements, and the allegation that BMO conducted a "[redacted]." (*Id.* ¶¶ 60, 67, 74.) The Counterclaims also allege that "[redacted]," which allegedly "[redacted]" and "prevented other customers from trading through Optionable." (*Id.* ¶¶ 61, 68, 75.)

A good pen tester knows that there is always more to things than meets the eye! As a final point on documents, you may encounter during the recon phase, be sure to look carefully at any that include redacted content.

On more than one occasion, we've come across redacted content that was not actually redacted. Especially in PDF documents, you will find that sometimes redaction is just a "cover up" for the text that is still there and can even be highlighted and copied for perusal in a new document. While this is definitely not the norm, never give up just because the content appears to be removed—sometimes it isn't.

Information Brokers

- Information brokers are usually commercial services for locating people and organizations' information
- Popular brokers include:
  - Acxiom
  - LexisNexis
  - DOCUSEARCH
  - Discreet Data
  - MasterFiles

A number of services are available (usually for a fee) that can help you track down much more thorough information sets about people and target organizations. Dubbed "information brokers," these services are used by law enforcement, private detectives, legal teams, and (of course) social engineers to find out as much as possible about targets and individuals. Common information that information brokers can provide includes birth records, marriage licenses, legal proceedings, divorce and other personal legal matters, criminal records, tax records, driver history and more. Some of the more popular information brokers today include:

- Acxiom
- LexisNexis
- DOCUSEARCH
- Discreet Data
- MasterFiles

Web Spidering

- While not purely "recon", spidering websites and looking for content is a smart activity to find directories and content that may be interesting later
- There are many tools you can use to spider websites and servers:
  - wget
  - Burp
  - ZAP
- Always look for the **robots.txt** file at the root of a web site!
  - Example: www.sans.org/robots.txt

```
User-agent: *
Allow: /
Disallow: /index.php/
Disallow: /get.php/
Disallow: /checkout/
Disallow: /app/
Disallow: /downloader/
Disallow: /js/
Disallow: /lib/
Disallow: /pkginfo/
Disallow: /report/
Disallow: /skin/
Disallow: /var/
Disallow: /shell/
Disallow: /tmp/
Disallow: /includes/
Disallow: /catalog/product_compare/
Disallow: /catalog/product/view/
Disallow: /catalog/category/view/
Disallow: /customer/
Disallow: /wishlist/
Disallow: /catalogsearch/
Disallow: /enable-cookies
Disallow: /no-route
Disallow: /poll/
Disallow: /review/
Disallow: /sendfriend/
Disallow: /tag/
Disallow: /newsletter/
```


Web spidering is another activity that you may want to pursue during the recon phase. While this starts moving us more toward traditional pen testing activities, the goal is simply to find online content and potential avenues of recon that you may not have realized. Most organizations' websites contain quite a bit of useful information and may also have a number of directories that contain documents, pictures, and other useful information that you can leverage.

There are many spidering and web testing tools available, but common utilities include Burp, ZAP, and wget.

When spidering or reviewing web content, be sure to check the robots.txt file for any content noted as "disallowed"! This is content that sites don't want search engine bots indexing, but to social engineers these parts of the site may prove valuable in gathering information.

Automating Recon

- Some of these steps can be automated, making the process of recon and target profiling much easier
- Common automation areas include:
  - Search engine browsing/queries
  - E-mail and phone number harvesting
  - Social media recon and profile harvesting
  - Website scraping/spidering

We've covered a lot of tools and techniques! However, some of them are manual in nature and can't be readily automated. Others can and we should always try to make our lives easier when possible, by automating searches and scraping data.

Some of the most common automation areas include:

- **Search engine browsing/queries**: Many tools can be used for automating search engine queries and looking for results. To get really granular, you'll likely need to sift through results manually at some point, but you can cut out some of the leg work with automation tools such as SearchDiggity, BingDiggity, and others.
- **E-mail and phone number harvesting**: Looking online for e-mail addresses and phone numbers is much easier with tools such as The Harvester versus using search engines and manually looking for juicy finds.
- **Social media recon and profile harvesting**: Recon-NG and other tools can greatly ease the pain of perusing social media profiles looking for useful pieces of information.
- **Website scraping/spidering**: Simple tools such as Cewl or more robust spiders such as wget and Burp can be used to gather information about targets from websites.

Analyzing Data: "Connectedness"

- Once you have gathered data about target organizations and people, you need to start mapping "connectedness:"
  - Personal/business relationships
  - Timelines and history
  - Related organizations/hobbies
  - Job roles/functions
  - Locations
  - Opinions/preferences

After gathering data about targets, you should now be in a position to sift through the data and build more in-depth relationships. These relationships, known in the realm of social engineering as "connectedness" allow for advanced campaigns to be put together. Some tools can help with this, notably Maltego. The goal is to develop all the "surrounding" data around your target, which may include:

- **Personal/business relationships**: Who does this person interact with? Do you know to whom the target reports at work? Who works on his or her team?
- **Timelines and history**: How long has the target been working at the target organization? How long has he or she been in the same role or been married? This kind of information can help you establish patterns of behavior and understand more about the target user in general.
- **Related organizations/hobbies**: What does the target do for fun? Does she have a passion for horseback riding? Does he love to travel and play golf? This information can help you craft the perfect, targeted phishing e-mail.
- **Job roles/functions**: What does the target do? If she's a programmer, perhaps she'll be interested in new development practices and could be enticed to read a blog post on the subject. If he's in finance, he might be interested in learning about a new book or course geared towards CFOs.
- **Locations**: Physical locations where targets work can help you to observe local behaviors and attempt media drops and tailgating attacks.
- **Opinions/preferences**: Many targets have strong opinions that they may voice online, helping you understand them better as well.

Building Profiles

- With a lot of data and sources, you may now be in a position to build an adequate profile for your targets
  - This is the ultimate goal of recon activities
- In-depth profiles are most useful for very targeted attacks such as spear phishing
  - For “wide sweeps” of phishing, media drops and so on, this is not as relevant

Once you have started to put together all of the pieces, you can build a profile of the targets. This doesn’t have to be 100% complete right off the bat—in fact, you’re likely to keep uncovering tidbits of information over the course of the engagement. However, you really want to spend time putting together a profile of your most targeted users, especially if advanced attacks like spear phishing attacks are planned.

If the majority of your social engineering exercises will be “wide sweeps” of users for simple phishing “click counts," then much of this detailed recon may not be as relevant. In our experience, showing targets just how much information is available online can sometimes have a dramatic impact on their risk perception.

Target Profiles

- A sample profile for a target may include:
  - Name(s)
  - E-mail addresses and phone numbers
  - Physical addresses
  - Family members/relationships
  - Hobbies
  - Affiliated organizations/causes

Target Name/Age	Target Company	Job Title / Role	Email Addresses	Phone Numbers	Location(s)	Sites/Domains	Family Names/ Relationships	Hobby 1	Hobby 2	Affiliated Organizations	Notes
JR Bob Dobbs, 40	Slack, Inc.	CEO	jr@slack.com bob@loungers.org	1.770.555.1212 1.404.555.3234	Atlanta, GA London, UK	www.slack.com slacking.wordpress.com	Betty, wife Miranda, daughter (13)	Slacking	Lounging	Laz-E-Boy	Bob is likely solicitation items

If you've successfully built a target profile by this point, you should probably have (at a minimum):

- **Name(s)**
- **E-mail addresses and phone numbers**
- **Physical addresses**: These are usually for work-related organizations and facilities, not for personal locations. We don't want to stalk people and this is usually outside the bounds of scoping and rules of engagement.
- **Family members/relationships**: People's families are NOT on the table for interaction or social engineering. However, if you can learn someone's family names or interests, this may prove useful in tricking them into opening an e-mail or visiting a site. Ethics play a very strong role in professional social engineering and you need to be conscious of using tactics that violate fundamental ethical principles. Although the real attackers may have no limits on how they perform social engineering, it's very unlikely that we'll be in that same position, even in advanced scenarios.
- **Hobbies**
- **Affiliated organizations/causes**

Once you've put together a profile, you're ready to get started planning the next phases of social engineering execution. Before we get there though, we've got one last point to consider (next slide).

Working with Legal and HR

- Because we're dealing with human beings, we need to be **very** careful about how we approach social engineering activities
- Coordinate with legal and HR teams beforehand to avoid:
  - Privacy issues
  - "Crossing the line" of professional ethics
  - "Hot button issues"

Be sure, before you get the tactical aspects of social engineering underway, that you have touched base with legal and human resources teams (or have done so via contacts at a client organization). It's very easy to unknowingly blunder into situations that can lead to legal or ethics violations if you're not careful. These may include privacy issues if you come across sensitive employee data, ethics concerns when performing recon and organization-specific "hot button issues" that you may not know about (usually political or related to other things going on internally).

Recon Conclusion

- Targeting and reconnaissance play a major role in more advanced social engineering campaigns
- Advanced attackers will spend significant time discovering information about specific users and organizational attributes
  - As pen testers, we need to do the same thing
- The amount of recon you engage in will depend on the types of activities involved
- Consider the SEC487 class dedicated to open source intelligence gathering (OSINT) for much more detail

This wraps up the reconnaissance and targeting phases of social engineering. There are many additional tools and sites that we just don't have time to cover! You could spend a significant amount of time on nothing other than recon and you will likely discover that most target organizations don't want you to spend this much effort profiling users, especially for basic phishing, on-site, and exploitation activities. For very targeted attacks, however, the likelihood of success is directly related to the amount of planning and reconnaissance work you do and sophisticated attackers know this well.

Depending on the types of social engineering activities you are doing, the amount of targeting will range from simple e-mail or phone number sweeps to much more detailed and rigorous individual-focused recon.

Consider the SEC487 class dedicated to open source intelligence gathering (OSINT) for much more detail.

Lab 1.2 - Recon and Profiling

Time Estimate: 30 minutes

In this lab, we explore some of the tools we've been discussing and put together a profile for social engineering activities.

Secure and Convincing Phishing

Phishing is a staple technique for social engineers. In this section, we review how to do it convincingly and securely.

An Intro to Phishing

- The “classic” attack vector
- Used in the days of emailed malware
- Still used in fraud campaigns and payload delivery
- The quality game has shifted though
- The most common SE engagement activity

Phishing is much the classic attack vector that cyber criminals have used to great effect over many, many years. It all started back in the days of emailed malware where an attached .zip or .exe would be sent with some moderately convincing mail message to trick the user to click. Today, it is still a go-to technique for scalable mass cyber crime and one of the primary vectors of initial attack, even in nation state or more skilled targeted attacks.

Most importantly though, this is the most common social engineering test activity. It provides us with a technique that can be used broadly across many systems and users at once and it involves minimal risk. When combined with other techniques, it often leads to excellent results, fast. It is, therefore, a technique we should know well—in this section, we explore what works and what does not.

Objectives

- What is a phish?
- What works?
- When phishing sets off the alarms
- Simple techniques to:
  - Bypass spam/boundary filters
  - Collect user data securely
  - Demonstrate potential for payload execution

In this section, we review what phishing is, how to do it effectively and what will set off the alarms and get you detected. We also review simple techniques to bypass spam filters, review some of the key technologies from anti-spam engines that will cause you problems, and how to create a phishing web page that tracks appropriate information securely.

Phishing is not hard to do, and it is remarkable how many users will fall for a moderately convincing snare (seriously, you often don't even have to try very hard). That being said, it is easy to inadvertently degrade the target's security with phishing and end up losing credentials that otherwise would not have been exposed. Let us go through how to perfect your phish and some scalable and simple techniques to customize your campaigns.

Secure Phishing

- Phishing is not necessarily hard, but we must avoid degrading security
- We need to create a suitable clone site or design a new copy (a clone is often easier and more convincing)
- We need to consider the legal, technical, reporting, and security requirements to make this work securely. There is more here for us to do than you would think!

Phishing is not necessarily difficult—indeed, it is often disappointingly easy. However, as ethical testers, there are a number of requirements placed on us that do not apply to the bad guys. Our objective is, of course, to create a clone site or design a new one that convinces the targets to hand over the required data. A clone is naturally likely to snare more individuals but sometimes we need to get creative and produce our own snare. Before we dive into this process, what additional restraints are placed upon us?

We need to consider the legal ramifications, the technical requirements, the data we wish to log (or should log), and we need a strategy to avoid degrading security. We explore each of these in greater depth.

What Is a Phish?

- A phish is a fake (typically spoofed) message that snares the user into behaviors such as handing over credentials or data, or opening system access.
- A phish is typically conducted over e-mail but it could be:
  - SMS /iMessage/WhatsApp
  - Voice phishing (or a vish)

A phish is essentially a faked message via some medium (typically e-mail but it could be any other) that snares the user into a behavior such as handing over credentials. There are variations on the term, such as vish, which stands for voice phishing.

Phishing is one of the most widely used mechanisms by attackers to collect user data (predominantly financial or credentials) as it scales and is low cost to engage in en masse. Let us go through some examples of typical phishing and how we might go about it as social engineers.

The Most Typical Phish

- Attacker crafts e-mail:
  - Contains a guise (we will discuss these shortly)
  - Typically, with a web link
  - A document-based payload also works
- The payload typically centers around:
  - Collecting credentials
  - Deployment of a backdoor
  - Simply tracking clicks

The most typical attack centers around e-mail. Typically, the attacker crafts an e-mail with some form of snare—a mail posing as a colleague, a fake UPS package delivery or a fake password reset request. This e-mail will typically include a web link where the objective is to collect credentials, deploy a backdoor or, in the case of a social engineering engagement, perhaps just collect clicks for reporting purposes.

Spoofing Mail

nc mail.server 25
Hello willingvictim.com
250 hello willingvictim.com
MAIL FROM:<james@willingvictim.com>
250 OK
RCPT TO:<test@willingvictim.com>
250 OK
DATA
Subject: Exciting opportunity
Dear Alan
.
250 Message queued

The slide shows a manual connection to a mail server in which we have supplied a MAIL FROM and RCPT TO command to instruct the mail server who is sending the message and where it must be delivered. In the old days of the Internet (and unfortunately some systems are still living in said days), you could pretend to be anyone and the mail server would conduct little or no validation about the truth of your claims. This made it trivial for phishing adversaries to send spam messages to their targets claiming to be from any site or user.

Today, the average user or business has a mail server and security software that introduces a significant number of checks and balances to prevent you trivially spoofing mail. One of the best strategies to deal with this is to use a legitimate e-mail server, a legitimate e-mail client, and a legitimate (albeit purpose-built for a test) domain. Why use hacking tools or risk generating odd headers when you can fall in with the noise of all the other good e-mails in the system? We discuss these mitigations in a few slides but, in some cases, you can just start up your own mail server and start sending mail to a domain claiming to be from another domain you do not own. Based on this, SMTP should probably be referred to as stupid mail transfer protocol rather than simple mail transfer protocol.

If you want to send phishing mails, again, we strongly recommend owning a domain for your phishes, as it will far more likely make it past filters than spoofed mail.

Getting Blocked? (1)

- Anti-spam
  - Typically focused on more mainstream spam
  - Encoded links can be a problem
  - Use a real mail client to avoid suspect headers
- Anti-malware
- Web filtering

There are many reasons that your phishing mail might be blocked but some of the most common are listed on the slide above. First, anti-spam and anti-malware can block phishing mail. These are pretty much a default in most modern organizations and, therefore, you need to know how to deal with them. The best line of attack with these particular technologies is to craft something custom each time and to minimize the surface area of detection.

Many anti-spam detection rules are based on abnormal data that a normal mail client or user would not include. Using a real mail client will drastically reduce the probability of suspect headers (or their respective omission). Using real domains and avoiding IP address-based links or complex URL encoding will also help avoid detection. A legitimate-looking e-mail, just like you would write to a colleague, will minimize detection from anti-spam technologies. I've rarely found it to be an issue in engagements.

Anti-malware is also simple to bypass with phishing. Typically, a link will go unnoticed, and it is only the inclusion of a nasty document or executable (or archive file for that matter) that can cause problems. If you must take this approach, a document that leverages built-in functionality such as macros are much less likely to be detected. Avoid the use of commonly available backdoors such as the Meterpreter however, as these are widely detected in OLE2 and .DOCX (and others in the family) formats.

Finally, endpoint- or network-based web filtering can be a pest. That being said, the majority of these controls operate on the basis of detecting malicious content (such as a payload) or based on the reputation of the site. If you register a legitimate domain name, use an SSL certificate and use a trusted hosting infrastructure such as Amazon EC2, the probability of being filtered is actually extremely small. I keep several legitimate sites as cover sites that I can use to run campaigns from—you might find the same useful if you frequently engage in these kinds of tests.

Getting Blocked? (2)

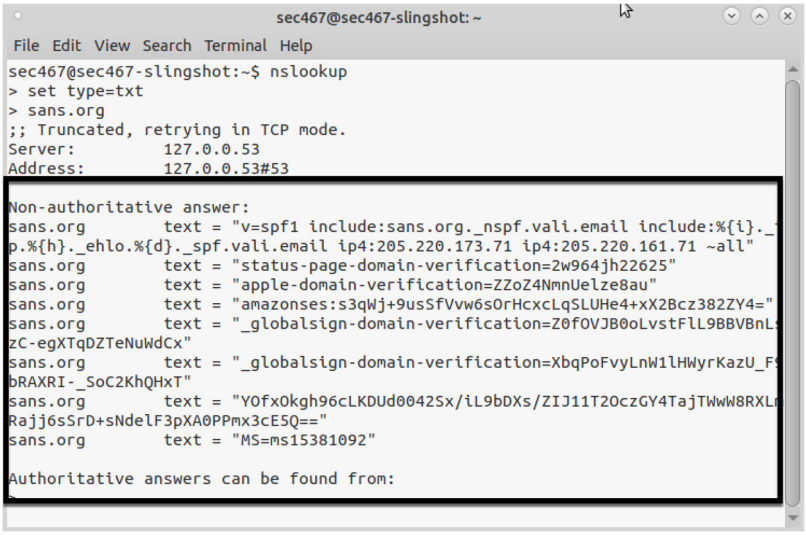
- SPF records
  - Sender Policy Framework
  - Receive validates sending host
  - Growing in deployment
  - RFC 7208
- DKIM
  - DomainKeys Identified Mail
  - Similar to SPF but validates mail has not changed in transit. Content-focused rather than envelope validation.
  - Not as widespread as SPF, but major providers use it

When conducting e-mail phishing, a number of additional controls can be troublesome. Sender Policy Framework is a mechanism (defined in RFC 7208) that enables a receiving mail host to validate that the sender is authorized to send e-mail on behalf of the sender domain. This rudimentary mechanism is actually effective at preventing you from spoofing known, legitimate mail-sending domains. This control works by having the receiving mail host do a DNS TXT-based lookup for a special SPF record. If you try and spoof e-mail for a host using these checks, it is likely the mail server will reject you. The best strategy here is not a complex attack but merely to use a sender domain that has a mail server that does not support SPF, or to use your own domain that looks legitimate (such as client-password-reset.com) instead.

DKIM is a complimentary control to SPF but less frequently used. DKIM instead focuses on validation of the integrity of the message and that the header and body have not changed in transit, whereas SPF focuses more on the envelope validation instead. The principles of bypass are the same—it is best avoided so choose from one of the many hosts out there on the Internet that does not support this.

Naturally, if the company does make use of these controls on their own domain and you need to send e-mail from that domain to a target, you are going to need to integrate this attack with other social engineering approaches to see success.

Detecting SPF



A quick DNS query can be used to identify if SPF is in use so that we know to avoid the domain. We simply execute:

```
$ nslookup
> set type=txt
> google.com
```

The section highlighted on the slide is the SPF record. The 'v=spf1' denotes use of SPF v1. Note the IP ranges—these are the ranges that are allowed to send e-mail. Also, note the ~all at the end of the SPF record. There are a number of policy stances that can impact your test:

-all (reject or fail them if tests do not absolutely match)
~all (soft reject; mark the mail as suspicious but accept it)
+all (pass regardless of a match)
?all (accept the mail, but can't weight negatively or positively)

Finally, note the include statement that tells the mail client to import the SPF records from another domain. If we query amazonses.com we will find a significant number of other IP addresses to be considered too. Already my social engineer spider sense is telling me to find another domain!

If we spoof a mail from sans.org to a server that supports SPF and it checks back with SANS, our mail will be rejected or at least aggressively quarantined. Of course, if we control DNS then none of this is an issue, but then we have already won. You can query domains until you find one that does not contain a record and these domains can easily be spoofed using the conventional methods. This is a far easier approach than butting heads with SPF.

What Gets You Blocked

- Suspicious links
  - Unusual domains
  - Strange encoding schemes
- Stereotypical bad grammar and spelling
- Complex guise in the message
- Closely replicating real-world samples
- Use of shared services or your own IP

There are a wide variety of things that can get your message detected or blocked, either by human detection or by security controls. Bypassing all of them requires a mixture of experience and luck but, to get you started, here are some of the most common problems.

Users have been slowly educated about the perils of suspicious links with odd encoding schemes. They have also been trained to keep a look out for rather stereotypical phishing messages that contain poor spelling and grammar. Cyber criminals, rumor has it, persist in using such poor-quality phishing because it roots out the users who are more gullible and more likely to fall for the later stages of their campaign. In a social engineering exercise where we are often emulating targeted attackers or operating in a shorter scale of time, we often want to aim a little higher and try to use more convincing samples. If we can get the organization to raise the bar to this level, then dealing with more opportunistic attacks becomes simple.

A great temptation when conducting these tests is to replicate real-world samples very closely. This is excellent as you do your company or customer the service of emulating real-world scenarios that they will need to defend against, and your report will show real exposure to real examples. The downside is that many security controls are geared toward reactive detection and, by the time you receive such samples and use them, they are relatively easily filtered. Inventing new but similar variations is a fair approach, as your goal should be to emulate the attacks in the first or second wave of use before mainstream security controls detect them trivially.

By the same measure, you should be cautious of using shared mail services that specialize in sending this kind of e-mail. A surprising number of these services have their IP ranges marked as suspicious or blocked and can drastically reduce the effectiveness of your campaign. The logical conclusion for many people is to then start up their own mail server instead; but operating from a cable modem IP range. Anti-spam filters also have plenty of mechanisms to pick this up and prevent your mail from being delivered. The best option is to behave like a real mail user but with nefarious intent.

What Works

- The infamous password reset
- UPS/FedEx/Amazon package delivery
- An HR incident (with caution)
- A simple calendar invite/share request
- Fake file transfers
- A colleague coming into town
- Company BBQ!
- All written as a first for your project, thus unique

There are so many different attacks that work, but some of my favorites are listed on the slide above. Your instructor will review these and likely add a few personal favorites also. Make sure you choose a scenario that matches the kind of data or access you are targeting, though it does not have to be an absolute match. I've often sent e-mails promoting an amazing company BBQ with great entertainment and some celebrity attending but with limited spaces. Employees are invited to click the link and register, but when they do they need to provide their internal network credentials to gain access. It is amazing how well it works in the majority of engagements.

You can go for fairly sinister approaches such as a fake HR incident, though I would recommend using this extremely carefully as it can lead to real altercations and fights. Better yet, keep it simple and pose as a file transfer where the target needs to enter credentials to accept a file or perhaps an Outlook Calendar link that poses as OWA and requires credentials for access. Any of these are less likely to strike personal chords and will see similar success rates.

If you craft each of these knowing the company well (its tendency toward certain acronyms or names of individuals in a position of influence, for example), you are far more likely to get clicks and avoid detection.

An Example

James

I'm coming in to town next week and have a really interesting client we should talk about face to face. Calendar link below. Choose a spot.

https://owa.corporate.tld/calendar.aspx?user=…

Dave

You can spend a lot of time making a clever e-mail with lots of graphics and nice finishing, but often the simple examples work very well. Take a look at this e-mail. It is forged from a colleague that quite possibly would send an e-mail like this. There is not enough to go on to immediately spot that it is fake, and the link looks moderately legitimate. It is even https:// and will have a padlock, which lots of users have learned to trust. This will have a relatively high conversation rate, but it requires greater customization than some of the other examples we have just discussed. Depending on the scope of your project, you may wish to go in either direction.

Naturally, when the target clicks this link, they will need to authenticate to access the corporate Outlook web access instance, right?

What Next?

- When a user clicks our link, we need to capture information. The typical next stages are:
  - Simply tracking the click for reporting
  - Collecting information such as a username/pass
  - Delivering a payload with greater functionality
- Typically, in social engineering engagements, the first two are the priority

Once we have crafted our mail and link, we need to prepare something for the user to be redirected to. This is where we collect information that supports our findings report. There are broadly three directions we can take at this point. First, we can simply log that the click occurred and identify the user, group, or IP address associated with it (more on that later). Second, we can produce a clone of an authentic site to collect information, such as usernames and passwords. Finally, we can deliver a payload that gives us greater control, such as a backdoor. Cybercriminals tend to focus on the third in the list (typically through the use of exploits for delivery, but sometimes by social engineering and asking nicely) but, as penetration testers, we are more interested in the first two. These show the organization its level of exposure without the enhanced technical risk of compromising a large number of systems. We review each of these approaches in greater depth in the coming sections.

Conclusions

- Phishing has many forms and variations
- Be creative but keep it simple
- Keep an eye out for security controls and spoofing defenses
- Where possible, use legitimate functionality and services to reduce suspicion
- When a user clicks, we need a payload

There are many different forms of phishing and even within the most well-known e-mail subcategory a million and one different styles of snare to try. Our advice to you is to be creative and try new approaches but keep it simple. Learning from the cyber criminals and echoing their tactics is usually a good approach—after all, our clients or companies want us to harden them against their efforts.

New security controls and mitigations are always coming in to play and often appearing moderately legitimate is the best way to work around these. Why fight anti-spoofing controls when for so little you can register a domain and send e-mails from it legitimately? We can then set to work on exploiting the human with our message and content rather than fighting over packet headers or trying to bypass DKIM checks.

When we do succeed there is an obvious next step. We need a payload for the user to click on and a mechanism to track them. Let's continue on to this challenge.

Tracking Clicks – Well, Duh

- SE engagements are often about clicks
  - Clicks on phishing e-mails
  - Clicks on suspicious executables
  - Clicks on suspicious documents
  - "Please open my USB nice receptionist?"
- We need a reliable way to track them on-scale without raising the alarm
- We also need the right level of detail for our client or management

Unsurprisingly, social engineering engagements are very often about clicks. It might be a click on a suspicious/unvetted link in an e-mail, or an executable or some other snare. However, if we manage to convince a user to do something they shouldn't, we need to know that they did it so that we can build a report for the client or management.

It is critical to social engineering engagements that we have a reliable way to collect this information and report on it without raising the alarm. More importantly, we also need to do it on-scale. In a social engineering engagement, you might execute more traditional penetration testing style attacks on one or two users (deploying a backdoor for example to collect data) but then much of the engagement is about demonstrating the breadth of the issue. We need to know that 367 users clicked on a certain campaign and 412 users from another separate division fell for a certain phishing campaign. This all needs to be captured at the right level of detail, although too much detail can be a bad thing.

The Right Level of Detail?

- This has happened many times:
  - Social Engineer: *"171 users clicked this phishing link."*
  - Executive: *"We need to fire these people or give them a formal warning for endangering the company. Please name the individuals."*
  - Social Engineer: *"Uhhh, two of them are sitting in this room."*
  - Executive: <<goes tomato red color>>
- Ratting out individual users is risky and often unnecessary
- This needs to be agreed in the scope and planning
- Can be legally tremulous too

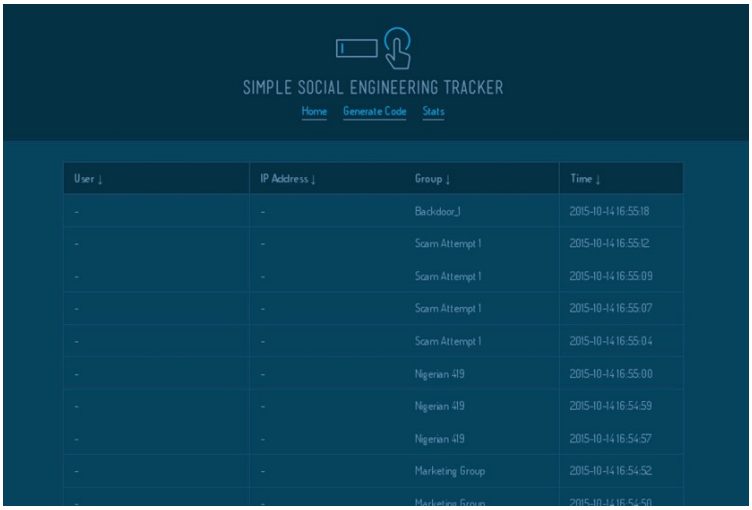
This is a conversation that as social engineers we have experienced way too many times and is one that you should try to avoid but will need to tackle head-on at some point. The executive team sponsoring your engagement (replace with CIO, CFO, CEO, or GC as you see fit) will want to know the exact details of these "sinners" who conducted bad behavior. In some situations, this might be the right thing to do but in most, it absolutely is not. This is a situation that needs to be dealt with delicately.

When you first start social engineering engagements or broader educational campaigns with a company, the chances are that a lot of people are going to fall for it. In most instances, you are doing it wrong if you do not get a decent percentage. There is little value in embarrassing or punishing people when we know that the enterprise has not done enough to help these people learn. It is better to understand the risk and take steps to mitigate it and improve the rate than to start naming and shaming. The above story is a good way to explain to executives that education phases should come first.

In some situations, it may be right to name and shame. What if you have executed several phases of testing and the company has heavily invested in quality education and you have an individual that is falling for everything? I once had a guy click on a phishing link 23 times in a row (once was enough really) to try and get his hands on a free iPhone (the phishing campaign was utterly terrible). At some point, people can become a risk that directly needs to be handled by the company. This is, however, not a process you should get involved with and the executive sponsor of your project needs to work very closely with HR. All of these issues should be discussed upfront in the scope and planning meeting. They can come as nasty surprises near the end of the project.

Another reason to be extremely cautious of this issue is data protection and privacy. Many countries have varying policies (as outlined earlier in the course) and avoiding collecting this information, let alone avoiding revealing it, can really help in avoiding legal pitfalls.

Introducing the Simple SE Tracker



This is the Simple Social Engineering Tracker. It is a tool we put together to make our own engagements easier and we built it up for this course. The Simple SE Tracker enables us to create tracking links, assign them to groups (for example departments or campaigns or both) and even collect some basic information from a payload, such as the username or IP address of the host. The code has a simple tracker script and an administrative interface that can build simple reports for management. Of course, there is nothing to stop you from exporting the data to a CSV to do your own pretty charts in Excel if you so desire!

Key Components (1)

- Tracker Script
  - http://10.10.78.1:8080/tracker/secure.php
- Admin Panel
  - http://10.10.78.1:8080/tracker/admin/
- Tracker Configuration file
  - /var/www/tracker/config.php
- Admin Configuration file
  - /var/www/tracker/admin/config.php

Next, we review the key components of the tool and what configuration parameters are available. These files can be edited to change the behavior of the tracker slightly, such as using a different decoy website. Naturally, these file paths can change if you install it on a different web server, but they should be relatively the same.

The Tracker Script
This script actually processes clicks or post backs. You can use this file name and a variety of others by simply copying and pasting the file. We have named it secure.php by default, as having secure in the URL strangely tends to make people feel happier about using the link. This file can be adjusted to track additional parameters with some rudimentary knowledge of PHP but, by default, accepts fields for username, IP address and the secure ID field that actually contains the tracking number. We will modify this shortly.

The Admin Panel
This is located in the admin subdirectory and is where you will find the web front end to generate new codes, track clicks, and generate basic reports. It does not implement a password protection mechanism by default, as you can simply use the web server or other tools to do this. Also, note it does not have to even be on the same server as the tracker; it just needs to be able to read/write to the database being used by the tracker. IP restrictions or crypto restrictions could even be used to limit access to this area. It does not need to stay in a directory named admin either as long as the files are kept together.

Tracker Configuration File
This file defines a couple of configuration variables that are key to the user experience (being tracked). It can change where the user is redirected when he clicks on a link that is correct, or if the link is corrupted in some way. This can be extremely useful for redirecting tracked parties to a decoy site that looks authentic.

Admin Configuration File
This simply defines configuration information for the administrative portal and is very similar to the tracker one.

Key Components (2)

- Tracker Database Configuration
  - /var/www/tracker/db.php
- Admin Database Configuration
  - /var/www/tracker/admin/db.php

Finally, you must configure two files for your local system: the Tracker Database Configuration and the Admin Database Configuration, both named db.php. You will need to configure your database connection string to work appropriately. By default, it is set to connect to localhost with a specified username and password, but you can adjust the connection string or database name as you require. You can even use it with Amazon RDS or another cloud-hosted database if you need serious scalability!

Initialization / Reset

- Initialization is now performed at container startup
- Container does not persist state between runs

In its current iteration, SSET will not maintain state between runs. When the container is restarted, the databases are dropped and reset.

Post Test Backup

- When you are done, you may want to keep your click evidence for your reports:
  - Copy web server logs (Nginx or Apache)
    Typically, /var/www/apache or nginx
  - Take a copy of the database
    mysqldump –u root –p social_engineering > client_backup.sql
  - The database can be restored later if you need to generate more reports
  - That database, or the backup, may also be queried by another tool

When you have completed a particular engagement, you may wish to keep a lasting copy of the results. This is not particularly difficult; simply take a backup copy of the web server logs (typically located in /var/www/apache or nginx) and a copy of the database. To make a database copy, execute the following command:

```
$ mysqldump –u root –p social_engineering > client_backup.sql
```

Hit enter when prompted for a password.

This file contains a complete copy of your results. If you want, you can restore this later to generate reports in the tool or to resume a campaign. Alternatively, you can use a different tool to import this data or query the database.

Ideal Setup

- A public web server (or company-wide routable server)
- A trustworthy domain or series of aliases
- /var/www/tracker/admin directory password protected, IP restricted, or perhaps only available to 127.0.0.1 requiring SSH tunneling
- Can separate admin/active functions to offline role

The ideal set up for a phishing exercise is to install the Simple Social Engineering Tracker on a public web server (or at least a server that is company-wide routable) so that every person in scope can reach it. This server should have a trustworthy domain pointed to it so that the links you generate can look legitimate, or perhaps even a series of aliases.

From a security perspective, the Simple SE Tracker should not hold particularly sensitive data but of course, you don't want to add to the problem and fail to practice security when it is precisely that which we aim to teach. The admin directory is where all the sensitive functions reside and should be configured as password protected. You can do this with the web server very simply. Alternatively, restrict the directory so it can be accessed only by 127.0.0.1 and then use an SSH tunnel to access it.

If you want, you can make your production server a copy of the tracker directory without the admin directory to limit the exposed functionality. Then, you can grab a copy of the database and use the admin tool and the database copy on your local system for security.

Lab 1.3 - Tracking Clicks

Identifying how many users clicked your nasty link and capturing relevant details

Now that we know how to do some basic phishing, let us generate some links that we can track, allowing us to measure who in the company clicks and which campaigns work.

Secure Phish Forms

Cloning legitimate sites and creating logging functions to capture your results

In this section of the course, we explore how to clone sites and generate captures and how to do it securely. As security professionals, we cannot afford to cause a data breach whilst attempting to educate staff.

Secure Phishing Forms

- So far, we have tracked clicks
- What if we need to capture data or pretend to be some other legitimate entity?
- We need to be able to clone sites or create our own simple capture pages
- As security professionals, we need to do this securely, so we do not cause a breach while attempting to educate staff

So far, we have just tracked clicks, but as part of social engineering engagements, we very often need to capture more information to really prove the impact of an attack. The most common scenario is capturing credentials or basic user information.

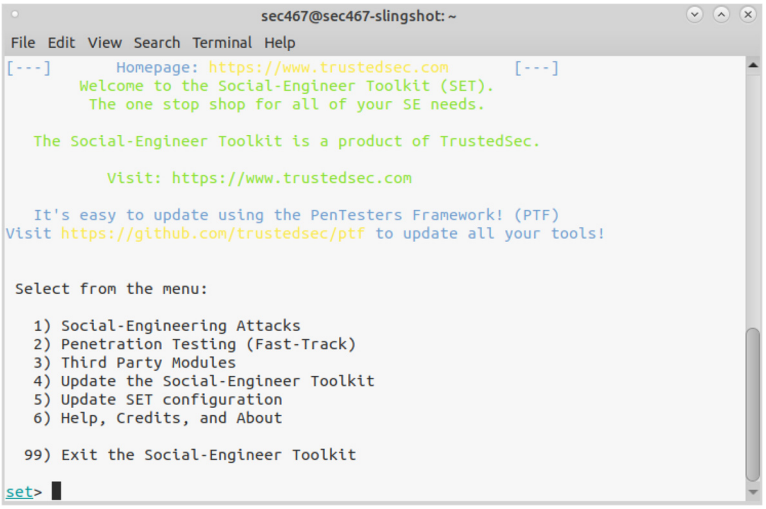
This is an area where we need to be very cautious, as there is the potential to violate intellectual property rules, data privacy or data protection rules and inadvertently name and shame users who need to be educated not shamed. We will explore all of these challenges in greater depth later, but regardless of these risks, it is key that we have the technical capability to make site clones or create our own capture schemes, otherwise our social engineering will not have a scalable payoff.

Goals

- Create a clone of a popular website that we can trick users into using
- Capture basic information, such as credentials from a form
- Roll our own concept capture site and log the data
- Carefully consider:
  - Use of https:// to avoid degrading security
  - What information we need to capture vs. what we should not capture for legal or ethical reasons

In this section, we will do two exercises. In the first, we use the Social-Engineer Toolkit to create a clone of a popular site so that we can capture information from users. In the second, we create our own simple capture/logging tool. This may seem like a strange inclusion in the course, but it is invaluable to be able to quickly roll something to fit the scenario you have developed and be able to live-monitor the results without using public services that might bleed the data or violate the legal terms of your engagement.

SET



The Social-Engineer Toolkit is an excellent toolkit with a myriad of tools to help social engineers. From generating payloads to configuring Arduino or Teensie modules to automatically type out payloads at pace, it is a treasure trove of functionality for social engineers.

The toolkit is the work of Dave Kennedy, or @HackingDave on Twitter, and it is produced by TrustedSec. In this next exercise, we use a specific function of it, but we cannot highlight enough how worthwhile the time spent browsing around this tool will be to a budding social engineer.

Lab 1.4 - SET Site Cloning

Cloning a website and serving it up as our own data harvester

In this exercise, we will explore one of SETs many functions and clone a website for phishing purposes.

Lab 1.5 - Data Logging

Rolling your own simple PHP data collector to log results

There are scenarios where other tools will fail or where we need to be able to customize our data collection tools. In these scenarios, it is invaluable to be able to build some quick tools or web assets to accomplish what we need.

467.1 Conclusion

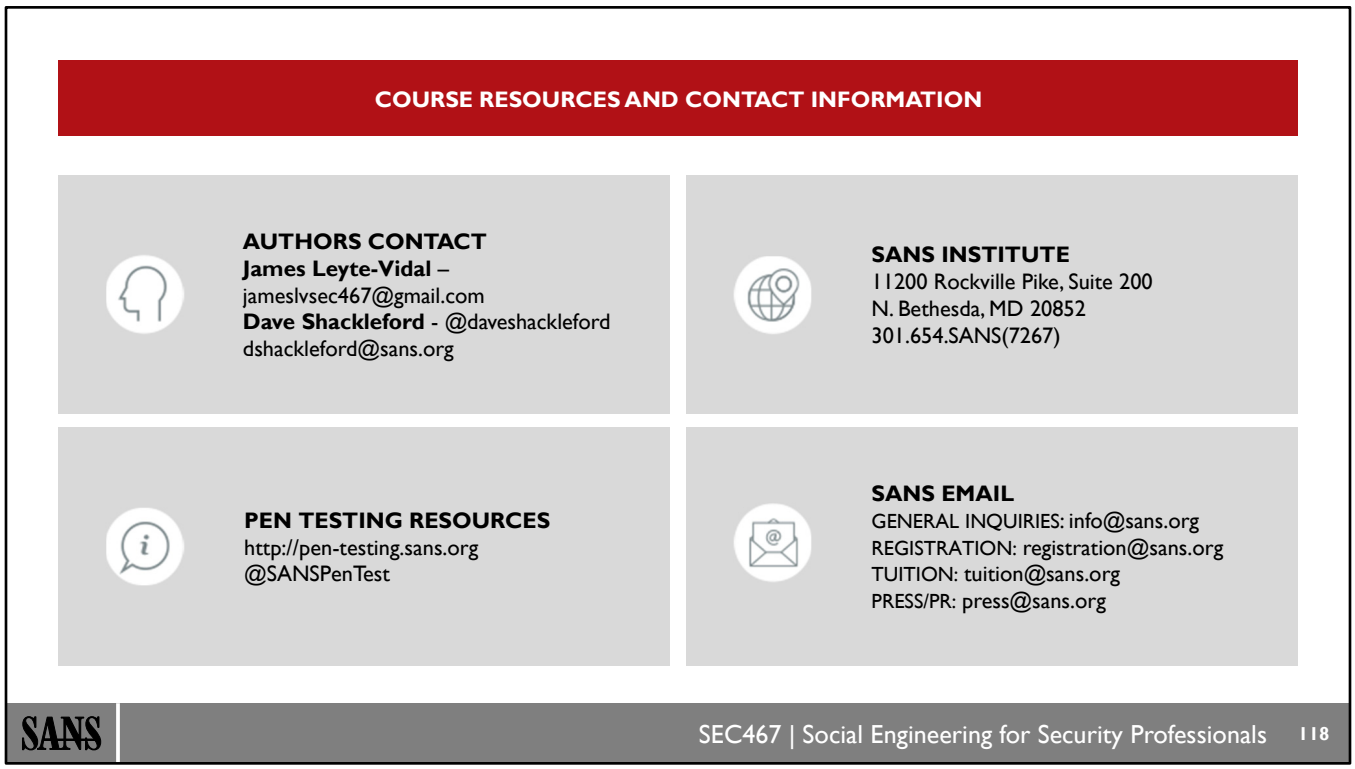
- Social engineering is more important than ever as part of an enterprise pen testing strategy
  - Attackers actively exploit people every day
- Numerous tools and sites are available for recon and profiling targets
- Phishing is one of the most powerful tactics in your arsenal
  - Ideally, both "wide net" phishing and spear phishing should be included

We covered a lot of ground in this section, between the motivation and psychology of social engineering to recon and phishing.

Pen testers have several tools and sites to profile targets and perform reconnaissance activities. Before getting started with phishing and other activities, it's best to spend some time upfront learning about your targets, finding information about them from public sources and developing profiles that can aid in your efforts and improve the success of your social engineering efforts.

As for phishing, it's definitely one of the most common attack vectors used by adversaries today and we need to emulate their attacks as much as possible. Both wide sweeps of employees and individual spear phishing targets should be phished, if at all possible.

Overall, it's key that enterprises understand how important social engineering is. As pen testers, we need to demonstrate where we're falling short and how attackers could take advantage of us.



This page intentionally left blank.