# Let’s Fire up our Engines : Information Gathering

Information Gathering is an art, the most important art of all , based on information , you make plans , you guarantee success and you take action , you if you don’t know the importance of information then you really have a series problem , There are many different ways of gaining access to information from a company. Some of the options available to a social engineer can range from using the telephone, intrusion within company property or using the Internet to obtain information. A social engineer can use many small pieces of information to combine into a useful vulnerability of a system. Information can be important regardless of its source , as long as it is related to your target ,each piece of text written , every word said is important .

# Methods of Information Gathering :

# 1-Research

Gathering information to support social engineering exercises is much the same as research you do for anything else. You need a goal in mind when you start in order to keep the research focused. Having a clear objective helps you determine what information is relevant to the end goal and what can be ignored. This holds true not only for the information gathered but also for how it's gathered.

## Social Networking Sites

Social Networking sites are now one of the most powerful weapons in the arsenal of a social engineer , whoever master the art of Social Networking information gathering , his life will me easier as a Social Engineer , Social Networks allow you to find tons of information about your target , his interest and his personal life , it allows you to get near him and you can organize a full scale attack on an organization based on using weak point in their system like a careless employee looking for love on facebook .

## Intrusion/Roleplay

Intrusion is considered actually entering the building or property of the target and obtaining information. Posing as an employee, an outside contractor, or even an IT administrator, the social engineer can ask questions or offer to fix issues

## False Websites - Phishing

Another way information can be obtained is to provide a website that looks legitimate for the company, possibly their own intranet site or a survey site that an employee would fill out. This site won’t take you to the real site, but will take you to a fake site that the social engineer owns The answers provided by the employee can give the social engineer the information they need to attain their goal.

## Tail Gating

Also referred to as Piggybacking, is where a person gains access to a secured building even if they have smart card passes or biometrics. Normal these can prevent unauthorized personnel from gaining access to systems and networks. People, unfortunately, are sometimes too helpful and will allow the ‘employee’ to enter in a locked door behind them because they are still searching for a pass that wasn’t there to begin with. The ‘employee’ running up behind the door before it shuts works just as well and allows for access to otherwise inaccessible places.

Shoulder Surfing

One of the easier ways of social engineering, simply look over the targets’ shoulder and a plethora of information can be obtained, commonly called shoulder surfing . Information obtained can range from user id’s to passwords to secret data seen in plain text.

# Dumpster Diving

Wikipedia defines dumpster diving as: "the practice of sifting through commercial or residential trash to find items that have been discarded by their owners, but which may be useful to the dumpster diver". The devastating nature of the items and/or information found can be anything from medical records, resumes, personal photos and emails, bank statements, account details or information about software, tech support logs and so much more. Of course all of this information can be used to leverage an attack against a victim.

Why does dumpster diving work?

The main reason for dumpster diving is for the acquisition of information. As with most forms of social engineering, "Working smarter, not harder" is a good slogan. Doing hours of work brute-forcing a password or account number that was discarded on an unshredded sticky post-in note seems silly when you can just obtain it from a trash bag.

# Traditional Sources of information

1. Corporate websites can provide a bounty of information. Spend some quality time with the site for your target and you can normally find information about the company, what they do, the products and services they provide, physical locations, job openings, contact numbers, bios on the executives or board of directors, and if there's a support forum there could be no end to the disparate nuggets sprinkled through the various posts.
2. A company's publicly reachable servers are also great sources for what they don't say. Fingerprinting servers for their OS, application, and IP information can tell you a great deal about their infrastructure. If you can determine the platform and application in use, this data could be combined with a search on the corporate domain name to find entries on public support forums. IP addresses may tell you if the servers are hosted locally or with a provider and DNS records can tell you server names, functions, as well as IP's.
3. Social media is a technology that many companies have recently embraced. It's cheap marketing that touches a large number of potential customers. It's also another stream of information from a company that can provide breadcrumbs of viable information. Companies will publish updates on events, new products, press releases, and updates that may relate them to current events (i.e. security companies telling how they can or already are protecting you from the latest vulnerability).
4. User sites such as blogs, wikis, and online videos may provide not only information about the target company, but also offer a more personal connection through the user(s) posting the content. A disgruntled employee that's blogging about his company's problems may be susceptible to a sympathetic ear from someone with similar opinions or problems.
5. Public data may be generated by entities inside and outside the target company. This data can consist of quarterly reports, government reports, analyst reports, earnings posted for publicly traded companies, etc.

Next Article We will discuss the concept of ELICITATION , that is how to extract information from sources