Social Engineering

The art of human hacking

# Chapitre 1 – A look into the World of Social Engineering

Qu’est-ce-que c’est le Social Engineering? Selon Wikipedia, “L'ingénierie sociale (ou social engineering en anglais), dans le contexte de la [sécurité de l'information](https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_de_l%27information" \o "Sécurité de l'information), fait référence à des pratiques de manipulation psychologique à des fins d'[escroquerie](https://fr.wikipedia.org/wiki/Escroquerie" \o "Escroquerie).” .

On peut dire que l’ingénierie sociale est la pratique de manipuler une personne à faire quelque chose qui pourrait ou ne pourrait pas être dans l’objectifs de la personne. Cette chose pourrait être obtenir une information, accès, ou une action de la personne dupée.

Pendant la vie quotidienne, nous rencontrons plusieurs types des ingénieures social, mais pas nécessairement ils sont négatifs. Ils sont :

* Hackers : ils utilisent l'ingénierie sociale pour obtenir accès dans systèmes parce que les softwares déventent toujours plus sûr.
* Penetration testers : ils utilisent l'ingénierie sociale pour aider le client à comprendre les défauts dans leurs softwares.
* Spies : ils utilisent l'ingénierie sociale pour duper les personnes et faire leur croire d’être quelqu’un autre.
* Voleurs d'identité : ils utilisent les informations obtenues par l’ingénierie sociale sur une personne pour se faire passer pour cette personne.
* Employés mécontents : souvent ils se revanchent après un licenciement en compromettant l’intégrité de données de l’entreprise.
* Escrocs : ils utilisent l'ingénierie sociale pour identifier les victimes idéales et attirer ces personnes.
* Recruteurs : ils utilisent l'ingénierie sociale pour comprendre la personne qu’ont devant.
* Vendeurs : ils utilisent l'ingénierie sociale pour identifier les besoins des clients.
* Gouvernements : ils utilisent l'ingénierie sociale pour contrôler les messages communiqués et les gens qui gouvernent.
* Docteurs, psychologues at avocats : ils manipulent les personnes à faire quelque chose qui ils veulent.

# Chapitre 2 – Informaton Gathering

Il n’y a pas une information qu’est inutile. Ce principe est très important.

Il y a beaucoup des sources pour recueillir des informations sur un objectif :

* Websites :
  + Search engines, par exemple en utilisant les « Google Dorks » (query strings : filetype, site, etc. : <http://www.googleguide.com/advanced_operators_reference.html>)
  + Whois Reconnaissance : on peut recueillir des informations sur numéro de téléphone, adresse, etcetera sur titulaires des services ([www.whois.net](http://www.whois.net))
  + Public servers
  + Social Media
  + User sites, Blogs
* Observation de l’objectif.
* Chercher dans la poubelle : souvent on jette informations sensibles sans les avoir disposés correctement.
* Profiling softwares.

Après avoir recueilli les informations, on les utilise en développant un modèle de communication (Communication Model).

La communication est l’action du transférer une information entre deux ou plus entités (émetteur et récepteur) par un médium. Lorsque l’information est reçue par le récepteur, il la décode et réponde (feedback). Toutefois, pendant une communication dans le contexte de l’ingénierie sociale, l’objectif est d’utiliser la communication pour créer un objectif commun. En fait, chaque personne décode l’information selon ses expériences, se humeur, ses perceptions. Donc, le devoir de l’ingénieure social est de comprendre l’interlocuteur et entrer dans se réalité et ses espace personnel : en fait, la communication n’est pas absolue.

Il y a différents modelés de communication (voir Shannon-Wearer modèle, Berlo modèle ou Balmand modèle), mais tous partagent la même structure :

1. Source
2. Channel
3. Message
4. Receveur
5. Feedback

Lorsque l’ingénieure social doit préparer une stratégie, il faut qui il analyse le modèle attentivement en prenant en compte les informations mentionnées ci-dessus.