Projet de SEN - Outils et simulation d'attaque

Mickael Bonjour

June 2020

Contents

1 Introduction

Ce projet consiste en 2 principales phases, tout d'abord la présentation de 3 outils puis sur une simulation/planification d'attaque. Les outils que je vais présenter son des petits outils qui n'ont pas forcément énormément de fonctionnalités mais qui sont à mon avis vraiment pratique. L'attaque est dirigée sur un conseiller fédéral suisse pour voir tout ce qu'on peut récolter sur une personnalité publique Suisse qui est très haut dans placé dans notre gouvernement.

2 Outils

2.1 wifiphisher

Introduction Outils permettant la mise en place simplifiée d'evil twin WPA en utilisant plusieurs techniques de phishing Wifi. Cet outil est gratuit et open-source[1]. Les développeurs encouragent les enthousiastes du développement python à améliorer la plateforme/proposer des nouveaux templates de phishing. J'ai choisi ce premier outil d'attaque car je trouvais intéressant de ne pas présenter un énième outil de phishing email, en effet le désavantage d'un outil comme celui-ci c'est qu'il est bien plus dur à mettre en place. En effet, il faut que la victime soit à proximité et que son appareil se connecte un peu automatiquement à certains réseaux. Cependant ça peut être vraiment intéressant si l'on sait que notre victime a par exemple pour habitude d'aller au Starbucks ou sur des wifis publics. Il est principalement testé sur la distribution kali linux, et étant une attaque Wifi il faut aussi s'assurer d'avoir une interface Wifi configurable en mode *monitor*.

Installation Comme dit auparavant il nous faut une distribution linux, sur kali linux wifiphisher est dans le package manager de bases :

```
$ apt-get install wifiphisher
```

Mais dans les autres distributions on peut tenter une installation depuis les sources :

```
$ git clone https://github.com/wifiphisher/wifiphisher.git
$ cd wifiphisher
$ sudo python setup.py install
```

[1] `https://github.com/wifiphisher/wifiphisher`

Description et capacités de l'outil L'outil a beaucoup de fonctionnalités et elles sont très bien décrites dans leur page github, je vais essayer de résumer brièvement et de présenter les principaux aspects de cet outil. Tout d'abord il permet de faire des attaques evil twin sur les réseaux détectés à proximité, puis de choisir quelle attaque de phishing l'on veut effectuer parmi celles proposées. Ensuite, l'on peut cibler un peu plus des noms de Wifis / noms connus dans des réseaux publiques par exemple. Cela pourrait nous permettre en se mettant à proximité des réseaux publiques de faire un evil twin et de proposer une sorte de plateforme de login via facebook et de récupérer potentiellement les identifiants de notre victime.

Exemples Je vais présenter ici le run de base que l'on peut faire avec wifiphisher uniquement mais comme décrit dans leur documentation l'on peut aller plus loin et faire des attaques KARMA, Known Beacons, evil twin; Pour commencer j'ai uniquement exécuter *sudo wifiphisher* et il va regarder automatiquement les interfaces disponibles pour l'attaque, de ce que j'ai vu une ne lui suffit pas, il en faut une pour le deauth et une pour l'evil twin. Cela va nous ouvrir une page comme celle montrée dans la figure 1.

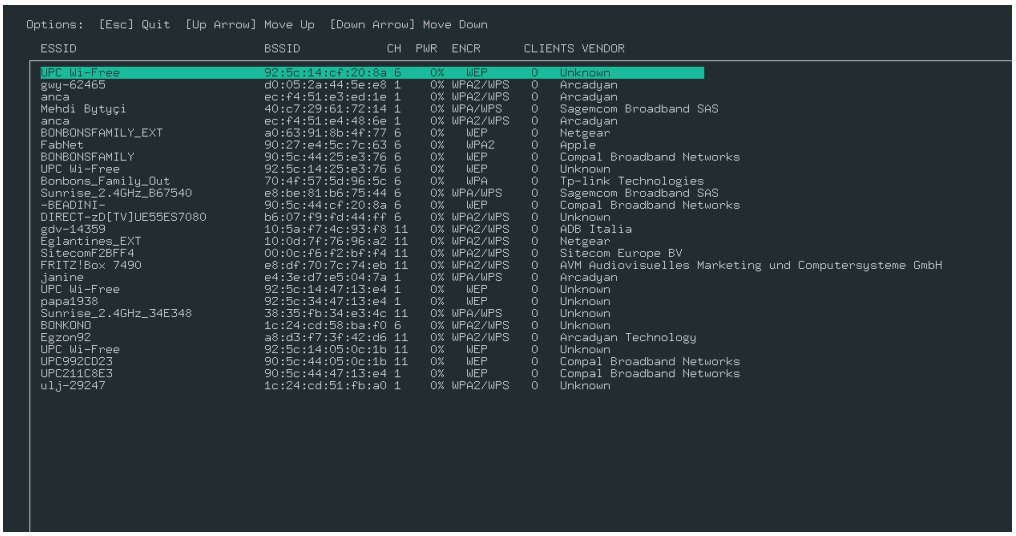

Figure 1: Choix du SSID à attaquer

De là on choisit le réseau à attaquer puis on choisit la méthode de phishing parmi ces 4 dans la figure 2.

Ensuite l'attaque se lance toute seule, malheureusement j'ai quelques soucis avec ma carte Wifi et le réseau n'apparaissait pas mais avec des adaptateurs adaptés cela fonctionne, ici un exemple de l'exécution finale dans la figure 3.

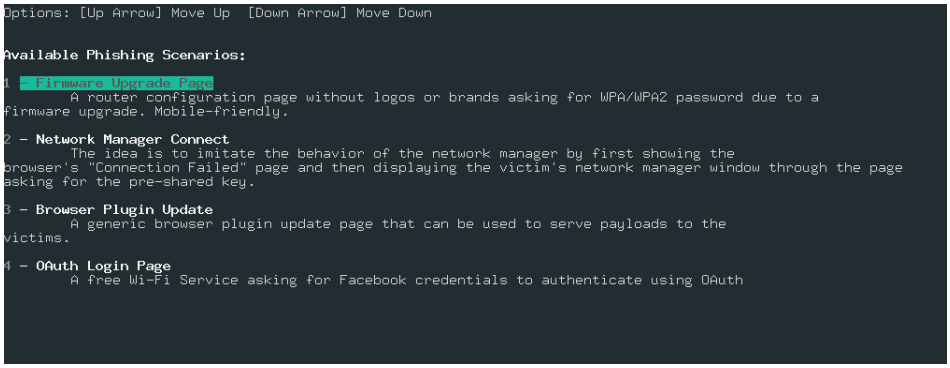

Figure 2: Choix de la technique du phishing

Figure 3: Sortie finale d'une attaque

Conclusion Je n'ai pas eu le temps de réellement finir le test et de voir de mes yeux la page de phishing mais j'ai mis cet outil en avant car il me parait simple d'utilisation et il est très puissant. Il faut juste un peu plus de recherches pour le dompter et trouver comment le faire fonctionner sur 2 interfaces puissantes, je n'ai en effet pas trop eu le temps ni le matériel pour effectuer tous les tests que j'aurais voulu.

2.2 LittleBrother

Introduction LittleBrother[2] est un outil de recherche OSINT orienté européen. Cela nous aide dans notre cas où l'on cherche plutôt des personnalités suisses/francophones. Il a plusieurs outils d'OSINT permettant la reconnaissance de personnes et un crackeur de hash de mot de passe. Ce qui est vraiment bien c'est qu'il ne requiert pas de login pour la recherche (facebook et Cie). Il est multiplateforme et intégralement en python, dès le moment où python3 est installé sur un système il fonctionnera.

Installation L'installation est assez simple du fait que ce soit un script python, il suffit de récupérer les sources, installer les dépendances puis de lancer le script.

[2] `https://github.com/lulz3xploit/LittleBrother`

```
$ git clone https://github.com/Lulz3xploit/LittleBrother
$ cd LittleBrother
$ python3 -m pip install -r requirements.txt
```

Description et capacités de l'outil Cet outil permet énormément de petites choses par rapport à l'OSINT d'une personne, l'on peut voir toutes ses options en le lançant comme montrer sur la figure 4.

L'on voit déjà un peu toutes les options de *lookup* que l'on a avec Little-

Figure 4: Menu lookup de LittleBrother

Brother, au niveau de la recherche sur une personne, de mail, de numéro de téléphone, traçage de mails. Mais il y a aussi la possibilité de créer des *profilers* et de leur créer des comptes en fonction des prénoms, noms donnés. Cela pour se faire passer pour quelqu'un d'autre sur les réseaux en recherchant des informations.

Exemples L'exemple que je trouve le plus utile de cet outil c'est la recherche google, c'est assez paradoxale de le faire via cet outil mais je trouve qu'il met bien en avant les liens intéressants comme montré sur la figure 5.

Sinon si on est en contact avec la cible, via des mails par exemple on peut voir depuis où le mail a été envoyé en combinant 2 fonctions de LittleBrother, le mail tracer et l'IP lookup comme démontré sur la figure 6.

Figure 5: Lookup google d'une personne

Conclusion Cet outil permet de faciliter nos premières recherches sur une personne et d'en apprendre plus sur ces comptes, et sur lui. Il est assez similaire au prochain tool que je vais présenter bien qu'un peu moins performant à mon goût, cependant il est plus orienté européen et de ce fait je voulais le présenter. C'est un avantage par rapport à la plupart des outils que j'ai vu jusqu'à maintenant qui se focalisait beaucoup sur des annuaires américains.

2.3 Buster

Introduction Buster[3] est un outil spécialisé dans la reconnaissance d'emails, je trouve que c'est important de présenter un outil comme ça car les emails ne sont pas très dur à obtenir de nos jours, de plus buster propose de récupérer l'email d'une personne en fonction de certaines infos qu'on lui donne et va tenter de reconstruire une liste d'emails possible et de les checker pour nous. Buster se présente sous la forme d'un programme python, il est possible de l'installer sur Linux. Par contre cet outil repose sur certaines API d'outil payant, ce qui fait que l'on atteint vite la limite fixée de recherche d'emails.

Installation L'installation de cet outil est très simple comme les outils que j'ai présentés jusque-là.

```
$ git clone git://github.com/sham00n/buster
$ cd buster/
$ python3 setup.py install
$ buster -h
```

[3] `https://github.com/sham00n/buster`

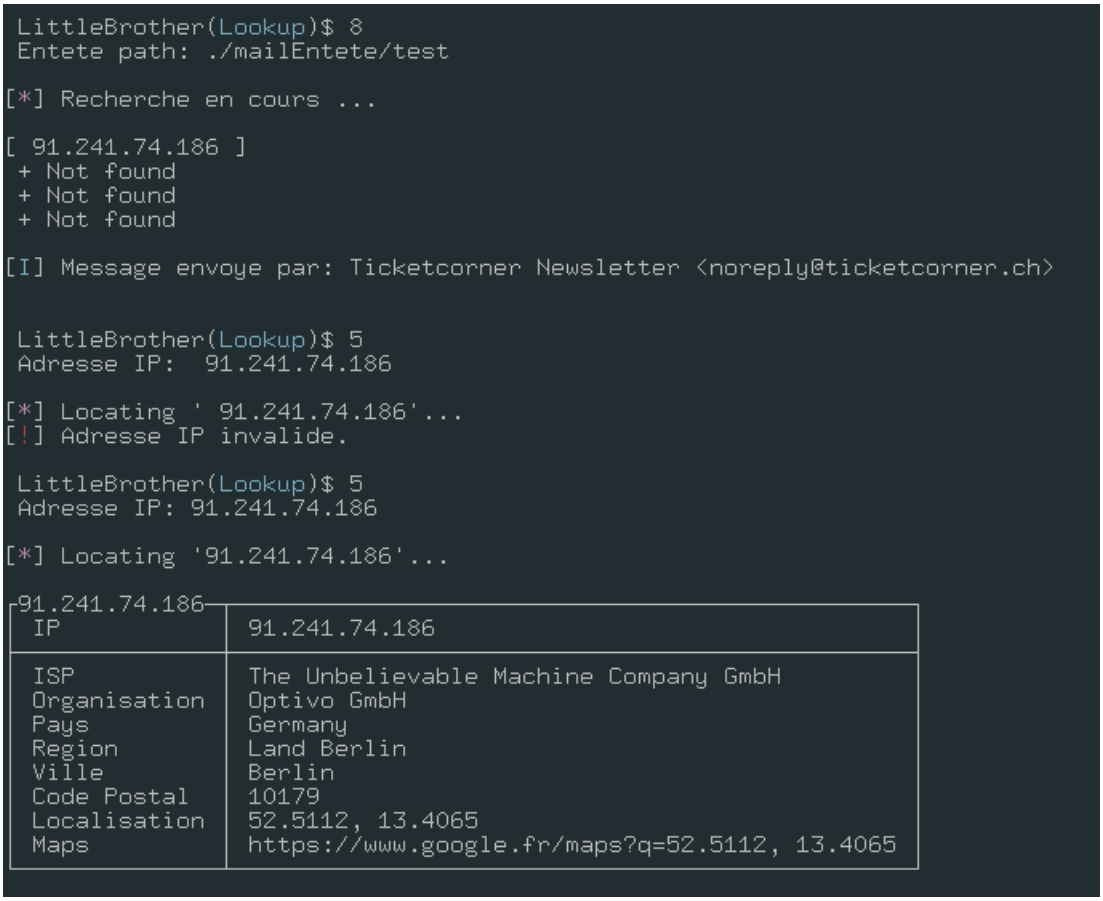

Figure 6: Mail tracer + IP

Description et capacités de l'outil Buster va aller chercher par le biais de beaucoup de sources si les variantes d'un mail existe est s'il est référencé sur un réseau social ou ailleurs, typiquement dans les brèches de données. Mais aussi chercher à l'aide de *dorks* google et voir où le mail apparaît. Il peut aussi générer les adresses des mails de travail et username en fonction des mails. Voir si l'email est utilisé pour une entrée DNS, ...

Exemples Pour présenter les capacités de Buster je vais essayer de lui donner plusieurs de mes mails et voir comment il réagit. Dans ce que j'ai vu il analyse bien les différents comptes associés à mes mails et ça me permet aussi de faire un checkup comme dans la figure 7.

Pour vous montrer les possibilités de variation dans les emails qu'il peut faire pour trouver le bon email j'ai fait comme dans le tuto proposé sur le github. Vous allez tout d'abord sur le profil de votre victime et récupérer son

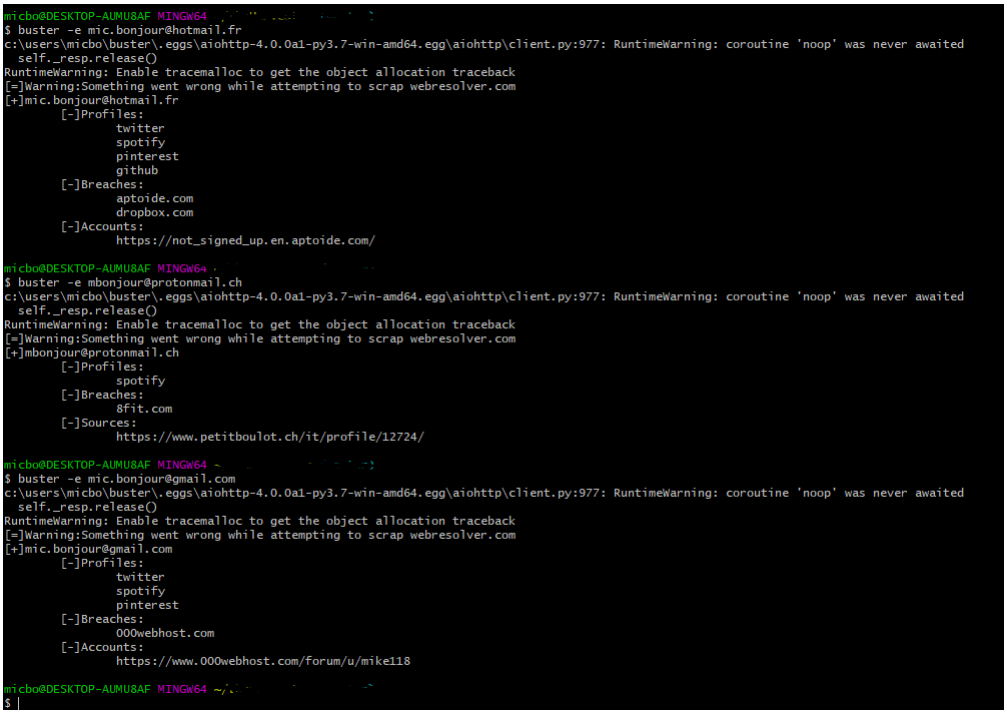

Figure 7: Exemple de run buster

ID/username dans l'URL, puis vous vous déconnecter afin de demander un nouveau mot de passe et vous mettez l'ID / username, vous allez avoir une fenêtre comme sur la figure 8 qui s'affichera, il vous suffira ensuite d'entrer les informations nécessaires dans buster afin qu'il cherche la bonne adresse mail comme montré dans le listing suivant. Je n'ai pas pu le tester sur moi car la limite d'essais s'atteint très vite et même avec un VPN pour augmenter le nombre d'essais le nombres valides d'emails à checker est trop grand pour la version d'évaluation.

```
$ buster -e m**********r@h*******.fr \
-f mickael -l bonjour -b ********
```

Conclusion Je trouve cet outil très pratique et facile d'utilisation, on le lance vite fait bien fait sur une adresse mail et il nous ressort des informations pour cibler nos recherches. Si l'on ne connaît pas l'adresse mail de quelqu'un on peut essayer de la deviner à l'aide de cet outil. C'est un petit outil simple et efficace.

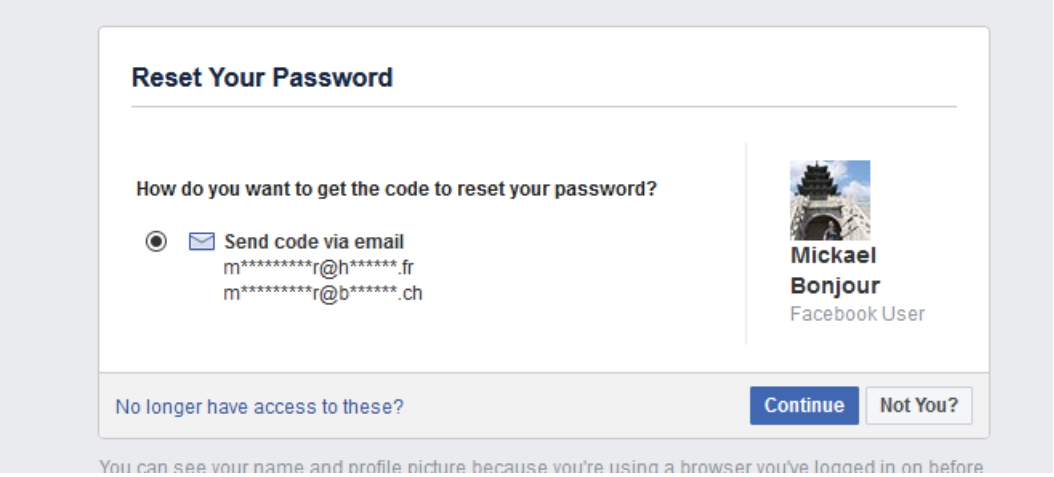

Figure 8: Exemple de run buster

3 Cible

Pour mon attaque j'ai choisi de cibler une personnalité connue comme suggéré, pour cela j'ai choisi Alain Berset notre conseiller fédéral qui a bien été médiatisé durant cette phase de confinement pour le coronavirus. Je trouve que ça peut être intéressant de voir à quel point les chefs de nos gouvernements se protègent et cachent leurs informations. Puis Alain Berset a été assez emblématique en cette période de confinement et il sera donc plus aisé d'en apprendre plus sur lui.

3.1 Recherche passive

Il y a beaucoup d'interviews et d'informations d'Alain Berset surtout dans ces temps de déconfinement. Voici un peu une liste des recherches faites et de leurs aboutissants :
Naissance : 9 avril 1972, Fribourg (48 ans) (Source : Wikipedia)
Sexe : Homme
Lieu d'habitation : Alain Berset, La Forge, Rte du Centre 35, CH - 1782 Belfaux, Fribourg (source : Google ,Wayback Machine[4])
Formation : Licence en Sciences politique et Doctorat en 2005.
Métier : Conseiller fédéral (Parti Socialiste Suisse), Chef du département fédéral de l'intérieur (Source : admin.ch)
Relations / Famille : Marié (Muriel Zeender Berset, Docteure en littérature française) et père de 3 enfants (Source: admin.ch)

[4] `https://web.archive.org/web/20060103210354/http://www.berset.ch/`

Personnalité : Personne impliquées dans de nombreuses commissions et associations avant son mandat de conseiller fédéral et pendant. Il montre une assiduité au travail de conseiller fédéral depuis 2012 où il a été élu. Par contre sur ces photos de rencontres il est souriant et émet un langage corporel sympathique. D'autant plus lorsqu'il s'occupe de son association *Les Buissonnets* dédiée aux enfants et adultes handicapés.
Biais d'attaques possibles : Twitter (@alain_berset), Mail (alain.berset@gs-edi.admin.ch), Facebook (géré cependant par une équipe et pas lui directement, inscription avec cet email : alain.berset@gs-edi.admin.ch). Il a aussi un site web qui est en fait un alias (www.alainberset.ch -¿ www.edi.admin.ch/edi/fr/home.html).
Points forts/faibles : Si l'attaque abouti a une prise de contrôle de son laptop il est possible d'avoir accès à des informations confidentielles conséquentes, voir même d'escalader dans le réseau du gouvernement. Il a 48 ans, Il n'est donc pas très âgé et connaît probablement assez bien les nouvelles technologies (il est inscrit sur twitter). Il est tout de même possible d'envisager une attaque mais elle ne sera probablement pas très facile. Sur le site admin.ch il est possible de demander une carte autographe avec la signature de M. Berset, je me demande à quel point il serait possible de se prendre pour le conseiller afin de faire une attaque au président p. ex. sur sa secrétaire.
Grâce à buster je vois que son profile facebook et Twitter utilisent cette adresse email, je pense donc que c'est son adresse email de travail, malgé l'avertissement sur Facebook nous disons qu'il y a une équipe intermédiaire. Sa femme n'est pas très active sur Facebook mais elle pourrait être un pivot pour atteindre notre cible.
Résumé : Au niveau personnalité Alain Berset à l'air d'être quelqu'un d'agréable et d'ouvert selon les témoignages de certains journalistes qui l'ont côtoyer. Malgré l'avancée médiatique qu'il y a eu pour lui il n'y a pas beaucoup d'interview personnelle qui en découle et je n'ai pas pu trouvé beaucoup d'informations en plus des informations publiques données. Au final il va être difficile d'attaquer Alain Berset en utilisant du phishing.

4 Scénarios d'attaque

J'ai pensé à plusieurs scénarios qui seraient potentiellement faisables et que je vais présenter ici brièvement. Le but principal étant toujours de voler un accès quelconque afin d'avoir potentiellement une escalade par la suite. En effet, vu la position de la cible il est plus intéressant de s'en servir comme tremplin vers le réseau gouvernemental.

- Typiquement aller sur le lieu de travail et essayer de repérer un café qu'il prend et d'attaquer via wifi public, peut-être pas efficace car VPN

pour se connecter au boulot, mais possibilité de récupérer d'autres identifiants via son téléphone peut-être ?

- Essayer d'aller lui parler en direct de façon bienveillante pour récupérer des informations, il est en effet médiatisé ces temps, ce ne serait probablement pas très louche.
- Essayer de proposer une interview comme si on était un journal officiel (*spoofcard* par téléphone, mise en place d'un site factice).
- Phishing en spoofant l'OFSP et informant d'un nouveau rapport sur le covid-19 avec trojan dans le rapport, typiquement fait à l'aide de metasploit pour intégrer un RAT dans le rapport en excel par exemple.
- Tenter de mettre clé USB dans le parking (vérifier s'il prend pas le train, je n'ai pas trouvé l'information dans la recherche).

Ce qu'il faut se rendre compte c'est que dans ces scénarios on a possibilité d'avoir accès à un réseau gouvernemental, c'est pour cela que je me dis que les attaques dirigées sur son travail ne sont peut-être pas une bonne idée à cause de sécurité probablement renforcée.

5 Simulation d'attaque

Je n'ai malheureusement pas eu le temps de faire une simulation d'attaque complète, j'ai essayé de proposer un maximum de scénarios qui me semblaient cohérent pour appuyer mes attaques probables. Cependant je n'ai pas fait de réelle simulation d'attaque étant seul dans ce travail cela aurait été difficile à mettre en place.

6 Conclusion

Ce laboratoire m'aura fait faire beaucoup de recherche d'outils, pour finalement prendre des outils assez simple et pratique d'utilisation. Cependant j'ai en tête beaucoup d'autres outils que j'ai analysés et tester (sur moi évidemment) tel que trape, phonia, spoofcard, theharvester... De plus, j'ai vu que l'on pouvait beaucoup apprendre d'une personnalité publique via la presse et des recherches finalement assez simples et très passives. Ainsi pour mon attaque il était facile d'établir un scénario plus ou moins réaliste. En étant seul sur ce travail je n'y ai probablement pas consacré assez de temps et j'ai donc dû réduire un peu la simulation de l'attaque et prendre des outils

un peu plus simple à analyser mais en restant intéressant. Je trouve le projet intéressant finalement et c'est sûrement mieux vu les circonstances actuelles mais j'avoue qu'avec le vote en début d'année je ne m'attendais pas un projet comme ça que j'ai trouvé trop conséquent par rapport à la matière. De plus sans cours ou presque dans le social engineering je ne savais pas trop comment m'y prendre pour trouver plus d'informations sur ma cible etc...