Etude et conception d’un botnet en python



**Team’s project ESD4**

Thomas GAFFET

Benjamin CAZIER

Ludovic CHOPIN

Année 2015-2016

Formateur : Jérôme Thémée

RNCP NIV I BAC+5

Expert en Sécurité Digitale

**Remerciements**

**Equipe Pédagogique**

*Jérome Thémée*

*Marion Bianchet*

*Julie Maquet*

*Charlotte Bergem*

Table des matières

1 - Note de cadrage 4

Identification du projet : 4

Phasage 6

Évolution du projet 7

Communication du groupe 7

2 - Les outils utilisés pour la réalisation du projet 8

3 - L'avancée journalière du projet 10

4 - Compte-rendu Kick-off Meeting 11

5 - La topologie 12

6 – La propagation - Le scénario du phishing 13

7 - Schémas de l'analyse fonctionnelle 14

8 - Le data flow 15

9 - La modélisation de données 16

10 - Le manuel d’utilisation 17

# 1 - Note de cadrage

Identification des parties, noms et coordonnées :

Organisme demandeur, interlocuteur : Ecole Aston

Équipe projet : CrystalMet (T.GAFFET, B.CAZIER, L.CHOPIN)

Tuteur : Thémée Jérôme

## Identification du projet :

Nom du projet : BOTNET

Nature du projet : projet mené par une équipe d'élèves dans le cadre de la semaine piscine

Ce projet a pour objectif de concevoir et d'implémenter un botnet en python, de fournir un livrable et une présentation de ce dernier.

Son objet principal est de proposer :

* une attaque DDOS à l'aide d'un trojan installé sur les machines zombies.
* Faire un « Reverse Shell » pour contrôler le zombie de notre choix.
* Faire une mise à jour du code source se trouvant sur le zombie.

Les enjeux pour l'organisme demandeur sont :

* Avoir un botnet fonctionnel.
* Fournir un livrable et une présentation

Les enjeux dans le cadre de la semaine piscine sont :

* Travailler en équipe.
* Réaliser un programme en python.
* Mettre en place une gestion de projet structurée.
* Valider la partie technique du cursus "Expert en Sécurité Digitale".

Son cadre général est le savoir être et savoir-faire autour d'un projet en équipe.

Ses contraintes principales sont :

* Le temps.
* Le manque de connaissance python.
* La coordination du travail en équipe.

Ses objectifs peuvent être ainsi résumés ci-dessous :

1. Le livrable papier qui comporte :

* la note de cadrage
* les outils collaboratifs
* L’avancée journalière du projet
* La topologie
* Le scénario de propagation
* L’analyse fonctionnelle
* Le data flow
* La modélisation des données
* Le manuel d'utilisation

1. Le code
2. La configuration du lab
3. La configuration du GIT
4. La réalisation du wrapper
5. Le ppt

## Phasage

Le projet est décomposé en tâches réparti dans un tableau kanban à travers les personnes de l’équipe projet ainsi que des listes de tâches « A faire », « A vérifier », « Terminé ».

- Jour 1

Thomas / Benjamin / Ludovic (Réunion kick-off, Répartition des tâches)

- Jour 2

Thomas (préparation du word, rédaction note de cadrage)

Benjamin (le data flow, la topologie du programme, la modélisation des données)

Ludovic (préparation du manuel du programme, le lab)

- Jour 3

Thomas (préparation du scénario de phishing, code)

Benjamin (code)

Ludovic (code)

-Jour 4

Thomas (Wrapper, ppt)

Benjamin (code, ppt)

Ludovic (code, ppt, démo vidéo lab)

- Jour 5

Benjamin / Ludovic (finalisation de l'ensemble de la documentation, présentation du projet)

## Évolution du projet

Si lors de la définition fine du projet, ou lors du déroulement du projet, il est constaté que des contraintes ne pourront pas être respectées, ou que certains des objectifs ne pourront pas être atteints, il en sera référé à l'organisme demandeur et au tuteur de projet, afin de décider des amendements à apporter à cette note de cadrage.

Livrable

Le projet botnet doit-être abouti, le livrable doit être remis le jour 5 avant la présentation du projet final devant le formateur et les autres étudiants du cursus ESD4

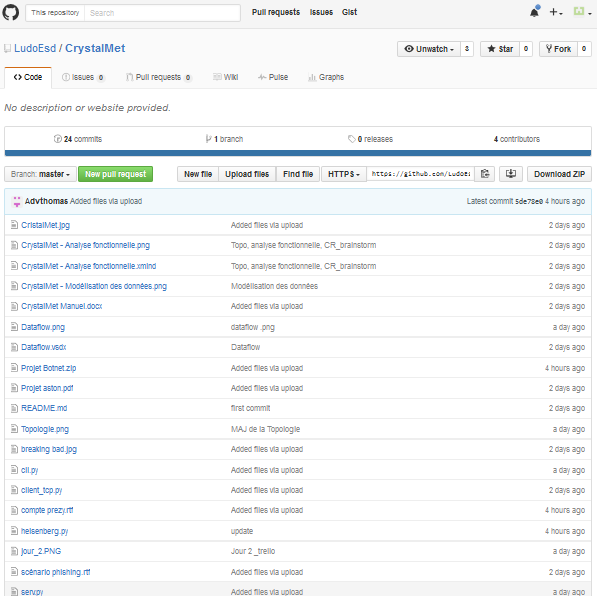
## Communication du groupe

La fréquence des réunions est au rythme d’une par jour afin de déterminer l'avancée des tâches de chacun et la validation des objectifs individuels au sein de l’équipe.

# 2 - Les outils utilisés pour la réalisation du projet

Utilisation d’outils collaboratifs comme :

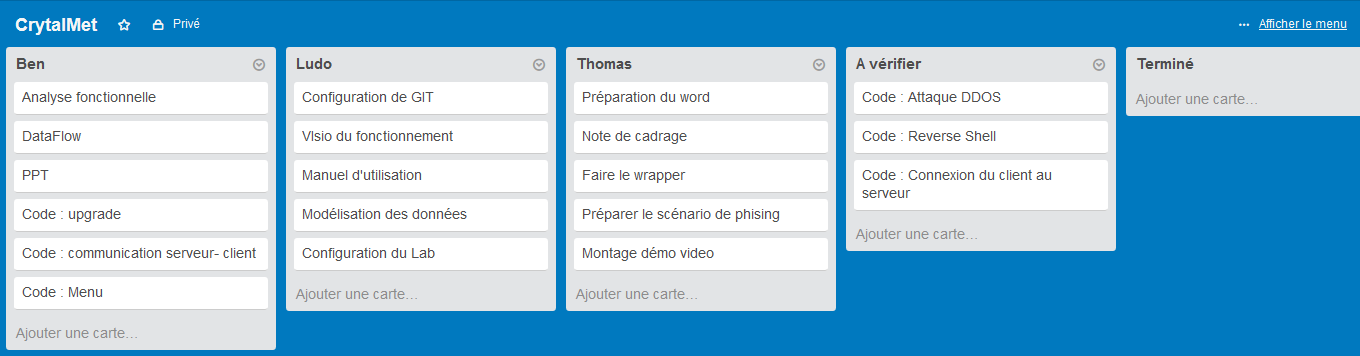
* Git : pour coder à plusieurs sur le même fichier et aussi comme dropbox (https://github.com/LudoEsd/CrystalMet)
* Trello : pour la répartition des tâches et travailler en agilité



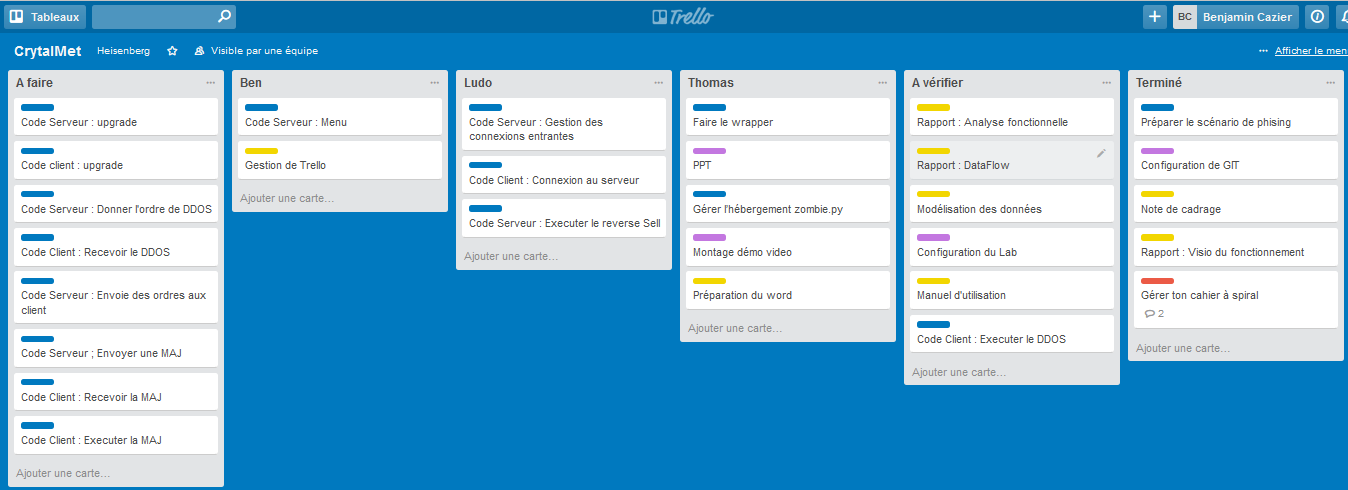
# 3 - L'avancée journalière du projet

Ci-dessous une capture d’écran de Trello, où on peut voir les différentes tâches réparties. Avec une liste par personne puis 2 files d’attentes « A faire » et « A vérifier » ou chacun peut pousser ou retirer des tâches.

Jour 1 :



Jour 2 :



On peut voir différentes couleurs :

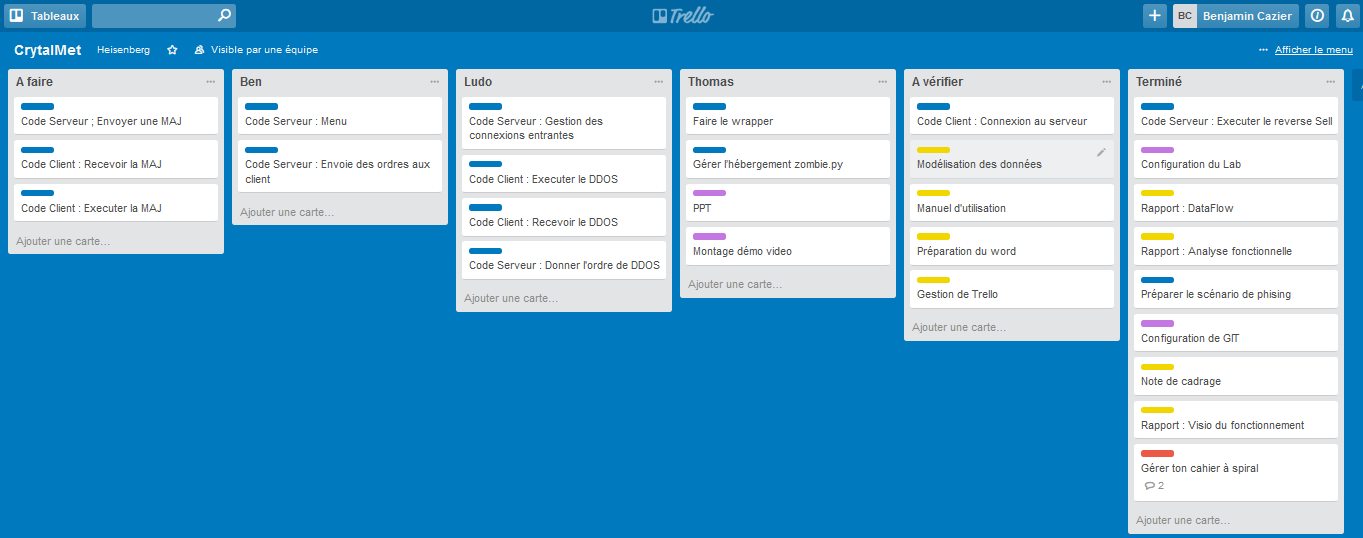
Bleu : Pour les tâches techniques

Jaune : Pour les taches du livrables

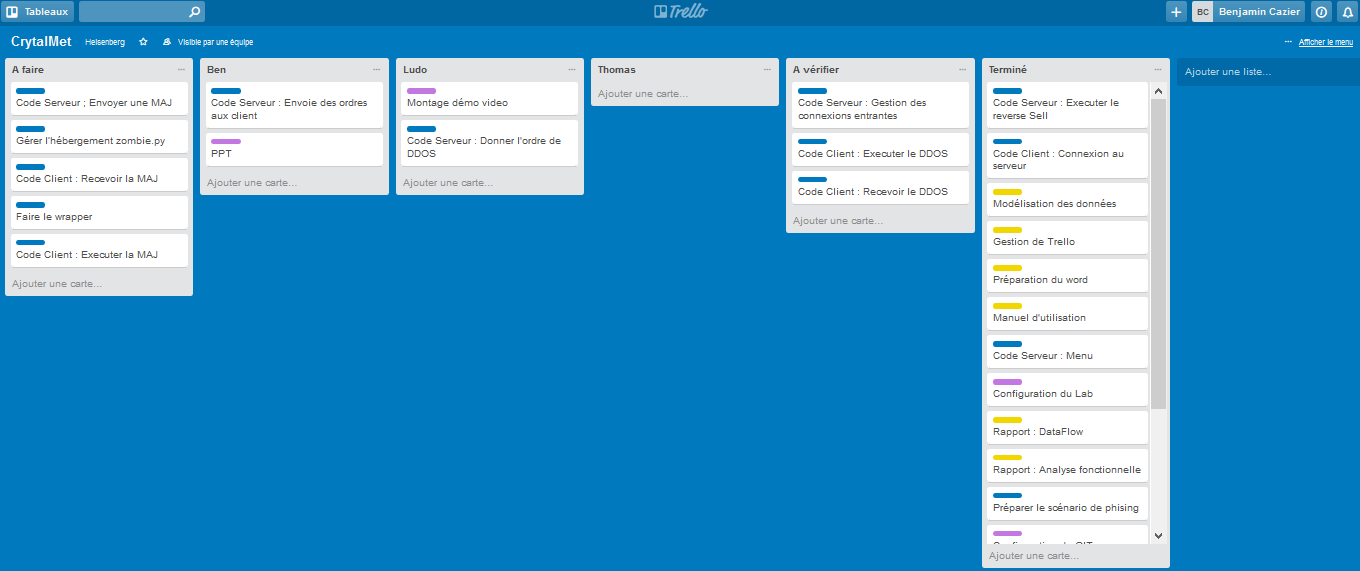
Violet : Pour les taches liées à la présentation

Rouge : Pour les trolls car faut bien rire un peu

Jour 3 :



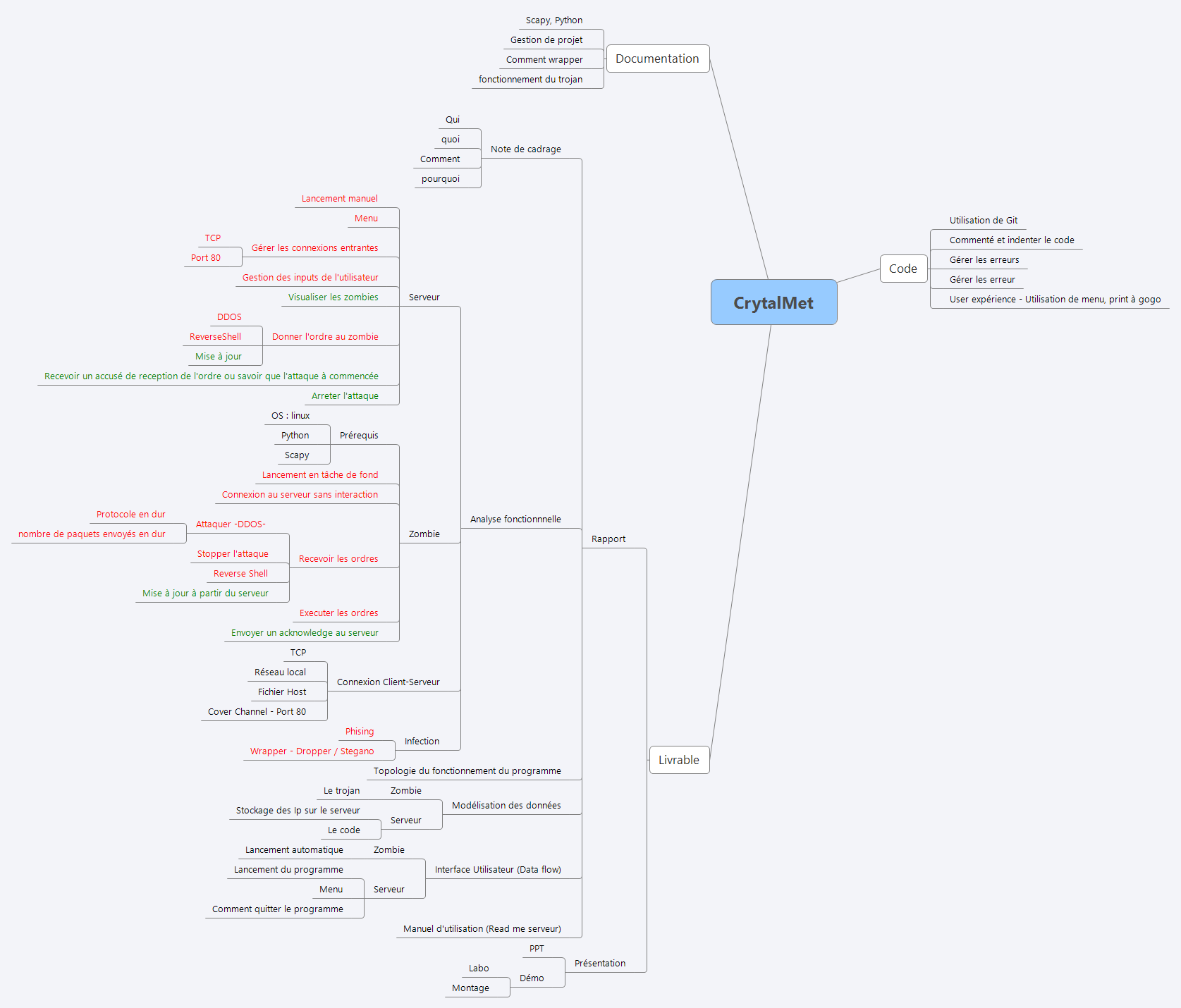
Jour 4 :



# 4 – Lancement du projet - Kick-off Meeting

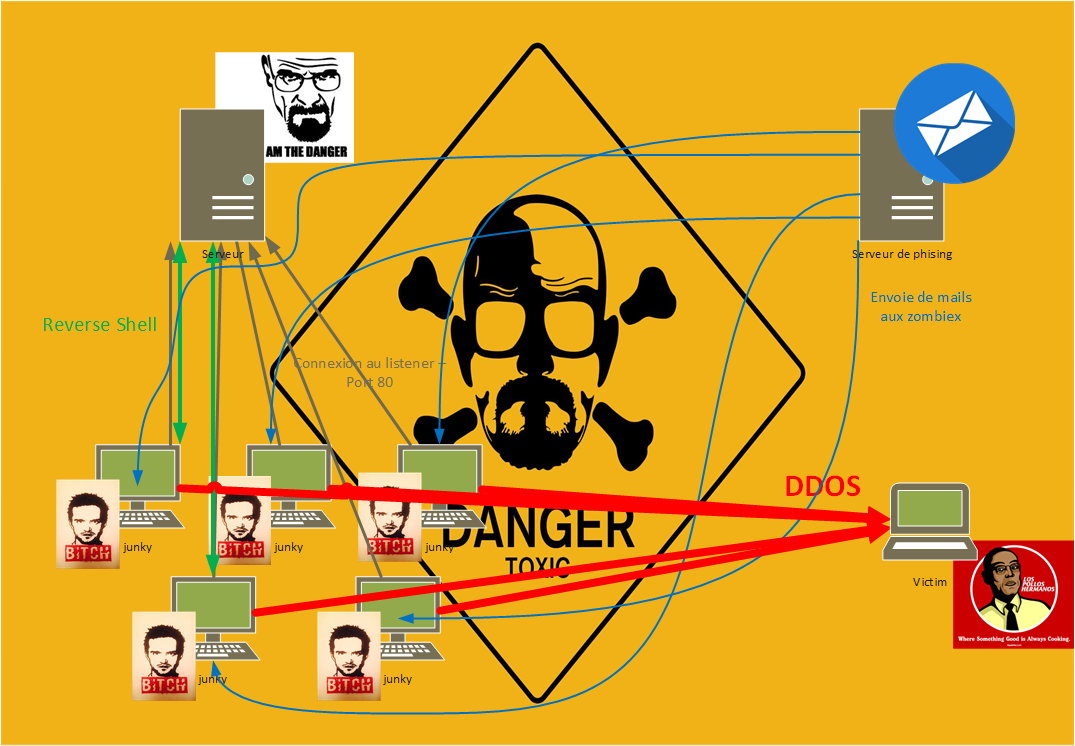
Pour le lancement du projet nous avons organisé un premier brainstorm où chacun envoyé les idées qui lui passaient par la tête sur chaque sujets évoqués.

Ci-dessous le compte rendu de cette réunion



# 5 – Fonctionnement du programme - La topologie

Nous devons créer un système qui soit capable d’infecter une machine sur laquelle nous pourrons nous connecter dessus pour effectuer toutes sortes de commandes systèmes. Cette machine servira également de zombie pour envoyer un DDOS sur une autre victime.



# 6 – La propagation - Le scénario du phishing

« « «

Annonce du film Breaking Bad par email à une liste de fan trouver sur les forums et sites de fan de la série.

Objet du mail: BREAKING BAD THE MOVIE

Vous êtes fan de Breaking Bad? L’oeuvre de Vince Gilligan ne s’arrête pas là!

Après 5 saisons à couper le souffle et déjà deux saisons du spin off qui met en scène l’ascension du célèbre “SAUL GOODMAN”, BETTER call saul! Vince pour les intimes à décider d’annoncer la préparation du film BREAKING BAD qui ni plus ni moins que la suite immédiate de la série! VINCE nous promet le film de sa carrière de réalisateur! En attendant la sortie de ce blockbuster, nous pouvons déjà admirer et saliver devant l’affiche officielle de cette pépite qui, je peux bien l’avouer, fait déjà palpiter mon cœur de rédacteur et de fan.

L’affiche ICI

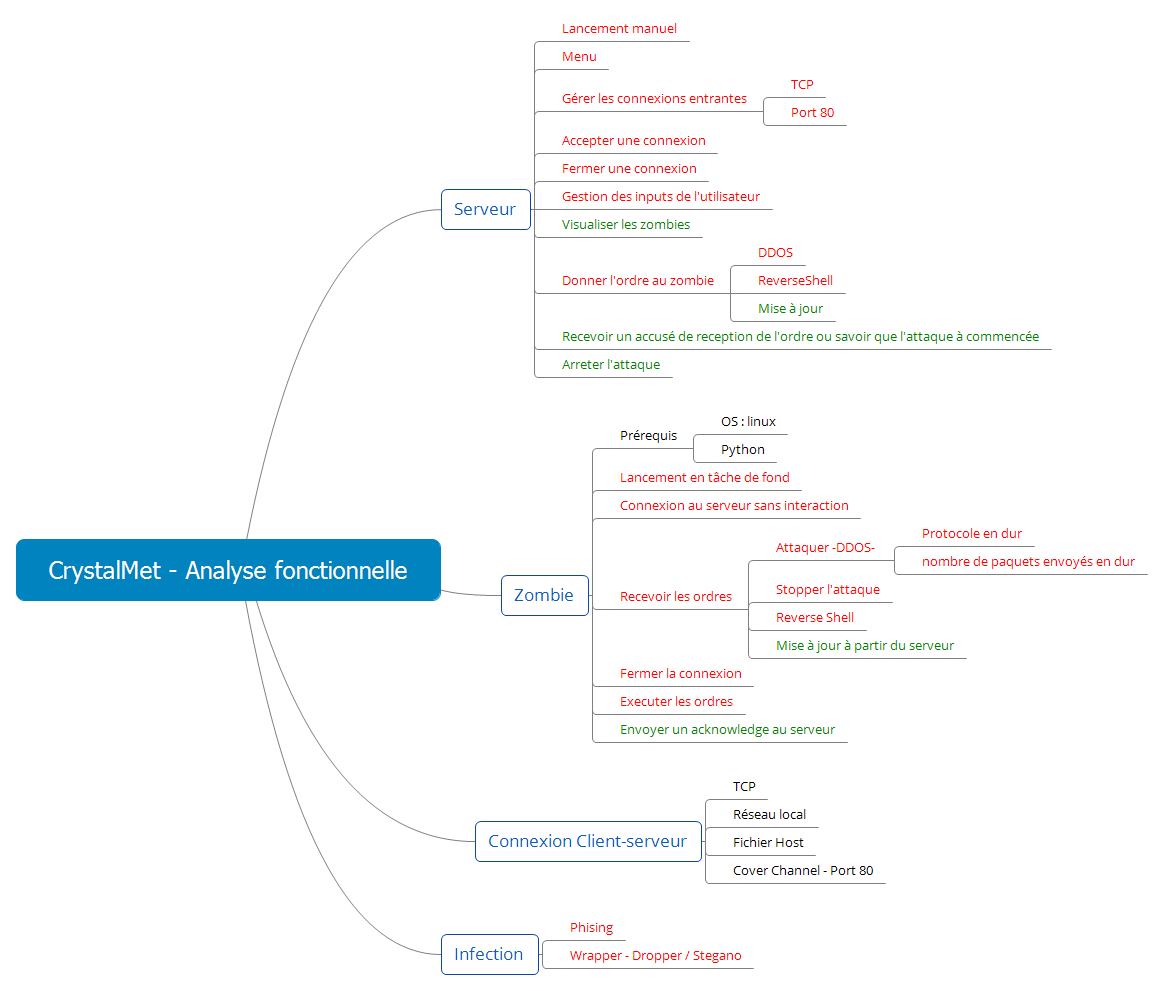


Utilisation de la sténographie pour cacher notre payload.py dans l’image de l’affiche. A l’ouverture de l’image le payload.py sera exécuté avec les droits de l’utilisateur.

# 7 - Schémas de l'analyse fonctionnelle

Voici la représentation de l’analyse fonctionnelle

* En rouge : les fonctions obligatoires, lesquelles nous tenons absolument à faire.
* En vert : les fonctions optionnelles que nous ferons une fois les fonctions obligatoires terminées.



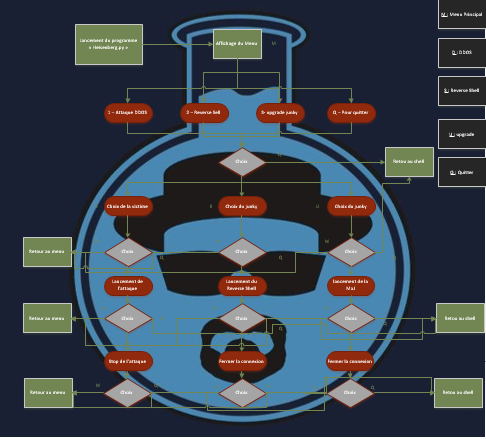
# 8 - Le data flow

Le data flow, voici la représentation schématique de l’expérience utilisateur avec le script principal.

L’utilisateur dispose de 5 touches pour naviguer dans le script :

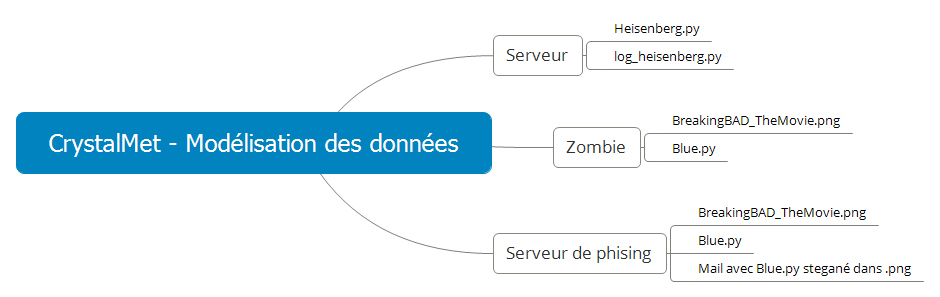
* M : Pour aller au menu principal
* D : Pour aller dans le menu de l’attaque DDOS
* S : pour aller dans le menu du Reverse Shell
* U : pour aller dans le menu d’upgrade du zombie
* Q : pour quitter le programme

Ces touches sont disponibles depuis chaque invite utilisateur.



# 9 - La modélisation de données

Voici la représentation schématique de la localité des fichiers du système :



# 10 - Le manuel d’utilisation

***CrystalMet***

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

The Botnet CrystalMet, Attaque Ddos, Shell et upgrade

**Description**

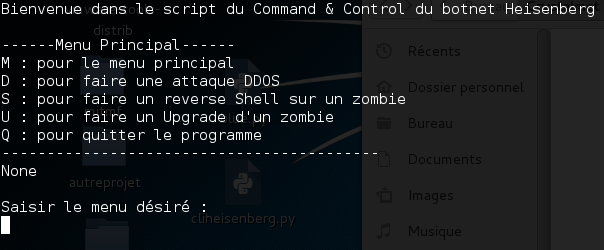
Le Botnet CrystalMet a pour but des fonctionnalités d’attaque Ddos grâce à des machines infectées (Zombie) ainsi que la possibilité de contrôler ces Zombies par l’ouverture d’un shell.

**Utilisation**

Le C&C doit être lancé prêt à écouter, afin que les zombies se connecte automatiquement.

Lors du lancement un menu s’affiche avec des taches à effectuer.

Pour plus de simplicité chaque tâche a été pensée avec une lettre qui référence une attaque.

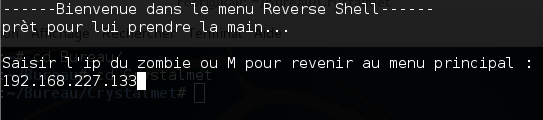


**Fonctionnalité du menu**

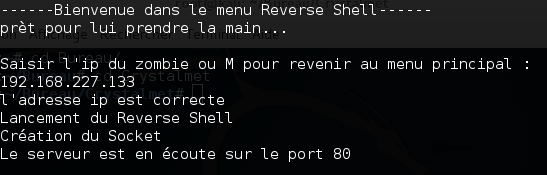
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Reverse Shell**

En tapant la lettre « s » pour shell reverse vous rentrer dans la fonction permettant le contrôle total de votre Junky



Le programme demande de taper l’adresse du junky connu du Command & Control, afin de s’y connecter, si l’adresse IP respecte le type d’adressage IP v4, alors le programme continue et ouvre la socket afin d’attendre le junky.



Lorsque que le junky se connecte, le programme vous demande de taper « 1 » pour lancer l’attaque.

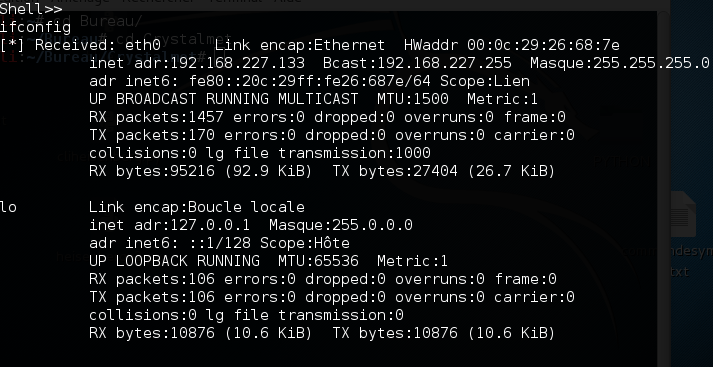


Taper « 1 ».

Le programme vous renvoie un shell sur le Junky.

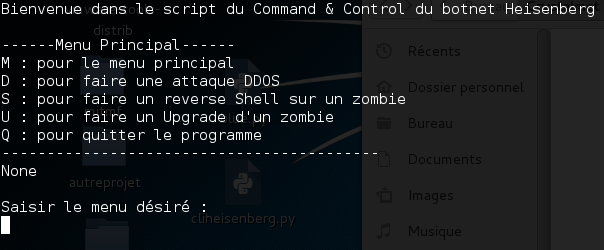


Vous pouvez désormais mettre à jour votre client « blue.py » depuis votre Reverse Shell ou exécuter les commandes de votre choix.



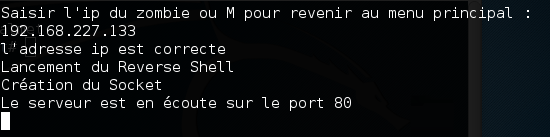
Attaque DDOS

Depuis le menu sélectionner une attaque DDOS en tapant « D »



Le programme demande de taper l’adresse du junky connu du Command & Control, afin de s’y connecter.

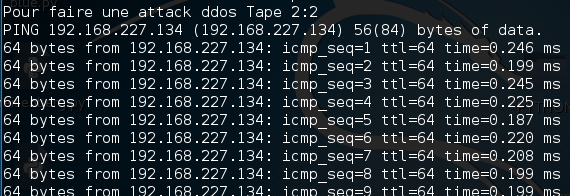
le programme continue et ouvre la socket afin d’attendre le junky.



**Dès que le junky se connecter le menu d’attaque vous propose de taper 2 pour lancer.**



**En tapant 2 l’attaque DDOS la victime.**



**Principe de Fonctionnement**