



Conception et exploitation d'un botnet avec Python



Team's project ESD4

GAFFET Thomas
CAZIER Benjamin
CHOPIN Ludovic

Ecole Aston

RNCP NIV I BAC+5
Expert en Sécurité Digitale

Année 2015-2016
Formateur : Thémée Jérôme



Remerciements

Equipe Pédagogique

*Thémée Jérôme
Bianchet Marion
Maquet Julie
Bergem Charlotte*

Equipe projet

*Gaffet Thomas
Cazier Benjamin
Chopin Ludovic*



Table des matières

Note de cadrage	4
Phasage.....	5
Fonctionnement	6
Évolution du projet.....	6
Compte-rendu Kick-off Meeting.....	7
Shéma de la topologie.....	10
Shéma de l'analyse fonctionnelle	8



Note de cadrage

Identification des parties, noms et coordonnées

Organisme demandeur, interlocuteur : Ecole Aston
Équipe projet : CrystalMet (T.GAFFET, B.CAZIER, L.CHOPIN)
Tuteurs : 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, d'implémenter un botnet en python et 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 et un main script sur un C&C pour contrôler les zombies, afin de mener une attaque de masse sur la cible de notre choix.

Ses enjeux pour l'organisme demandeur sont les suivants : l'école souhaite avoir un botnet fonctionnel ainsi que sa méthodologie à travers un livrable.

Ses enjeux dans le cadre de la semaine piscine sont : Savoir mener un travail en équipe, réaliser un programme en python, mener 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, les fonctionnalités python, la mise en place du projet global.



Ses objectifs peuvent être ainsi résumés ci-dessous :

- le document word
 - la note de cadrage
 - l'analyse fonctionnelle
 - la modélisation des données
 - le data flow
 - topologie
 - l'avancée journalière du projet à l'aide de l'outil Trello
 - préparation du scénario de phishing
 - un manuel d'utilisation
 - les outils collaboration
- le code
 - configuration du lab
 - configuration du GIT
 - réalisation du wrapper
 - le ppt
 - Montage démo vidéo

Phasage

Le projet est décomposé sur trello avec l'ensemble des tâches alloués aux trois personnes dédiés au projet.

- Jour 1

Thomas / Benjamin / Ludovic (élaboration de la note de cadrage et l'analyse fonctionnelle)

- Jour 2

Thomas (préparation du word, rédaction note de cadrage)

Benjamin (préparation data flow, topologie du programme)

Ludovic (préparation du manuel du programme, le labo, modélisation des données)

- Jour 3

Thomas (préparation du scénario de phishing, code)

Benjamin (code)

Ludovic (code)



-Jour 4

Thomas (Wrapper, code, ppt, montage vidéo)

Benjamin (code, ppt)

Ludovic (code, ppt, démo vidéo lab)

- Jour 5

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

Fonctionnement

La fréquence des réunions est au rythme de une par jour afin de déterminer l'avancée des tâches de chacun et la validation des objectifs individuels au sein du team's project.

Évolution du projet

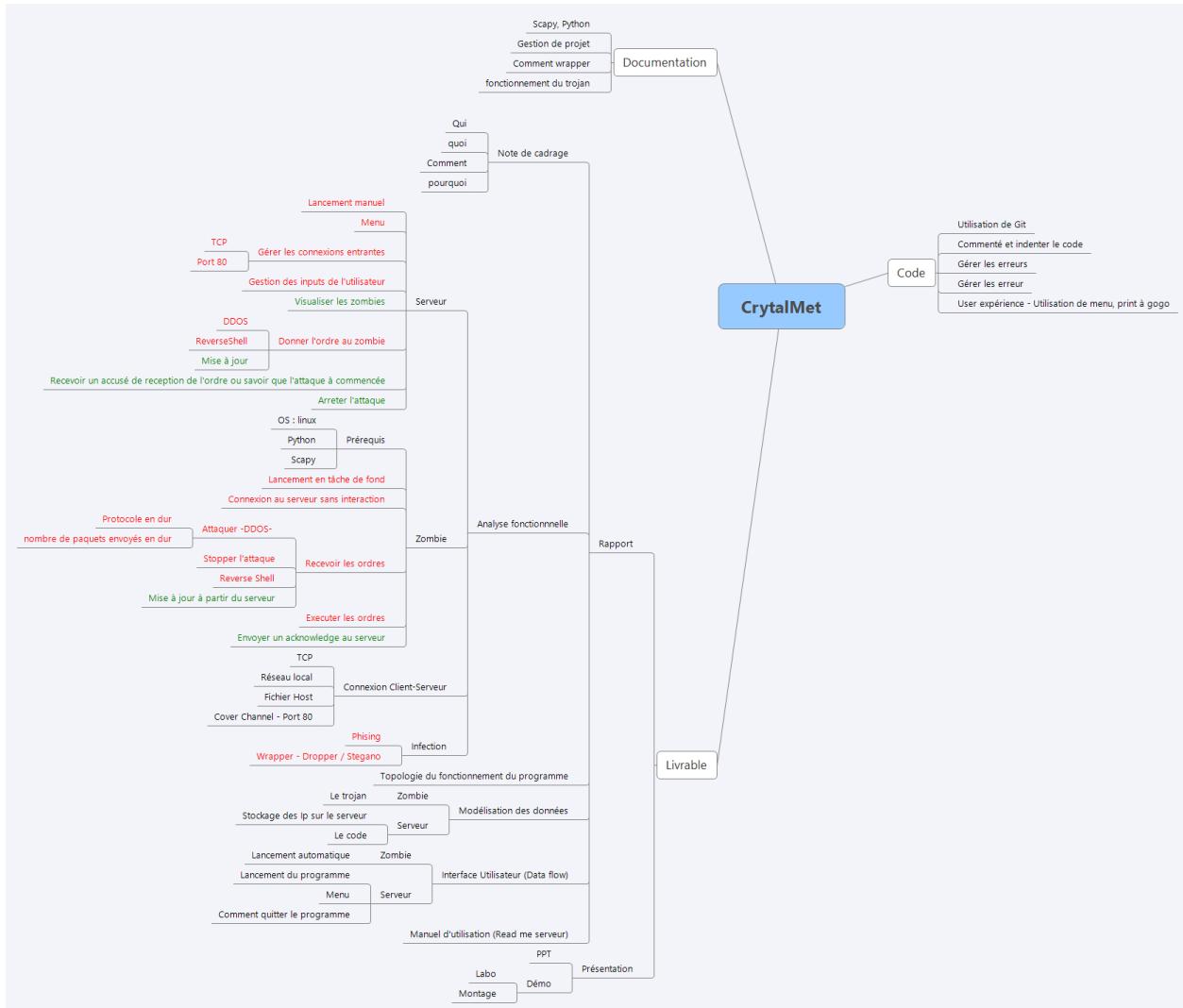
Si lors de la définition fine du projet, ou lors du déroulement du projet, il est constaté que des contraintes ne pourront pas être respectées, ou que certains des objectifs ne pourront pas être atteints, il en sera référé à l'organisme demandeur et aux tuteurs de projet, afin de décider d'un commun accord 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

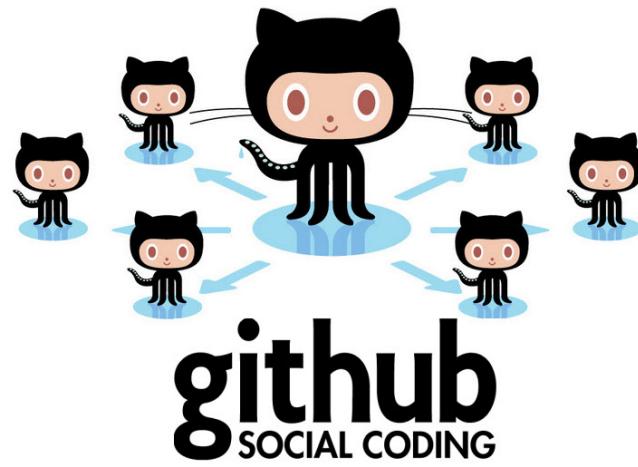


Compte-rendu Kick-off Meeting



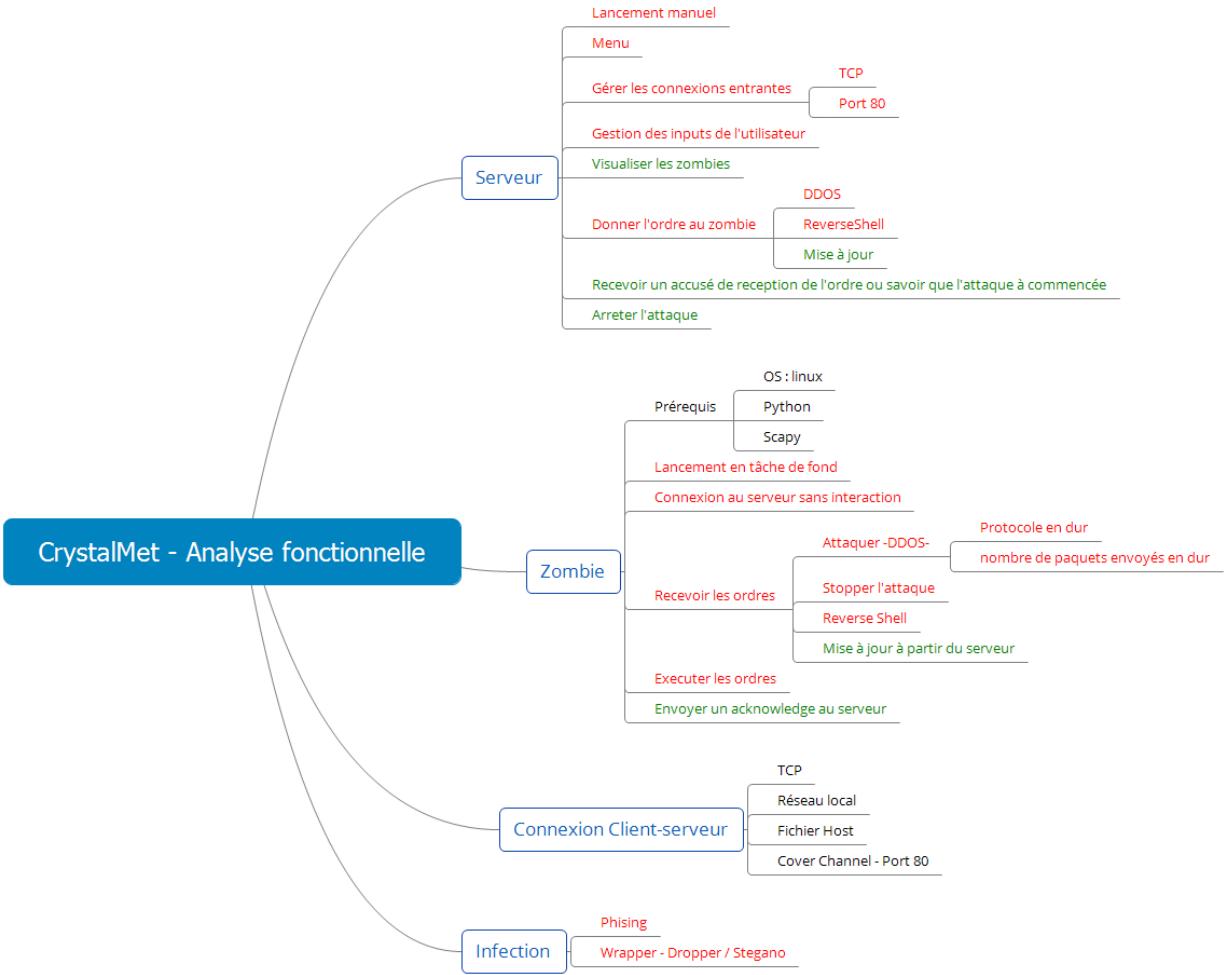


Les outils utilisés pour la réalisation du projet



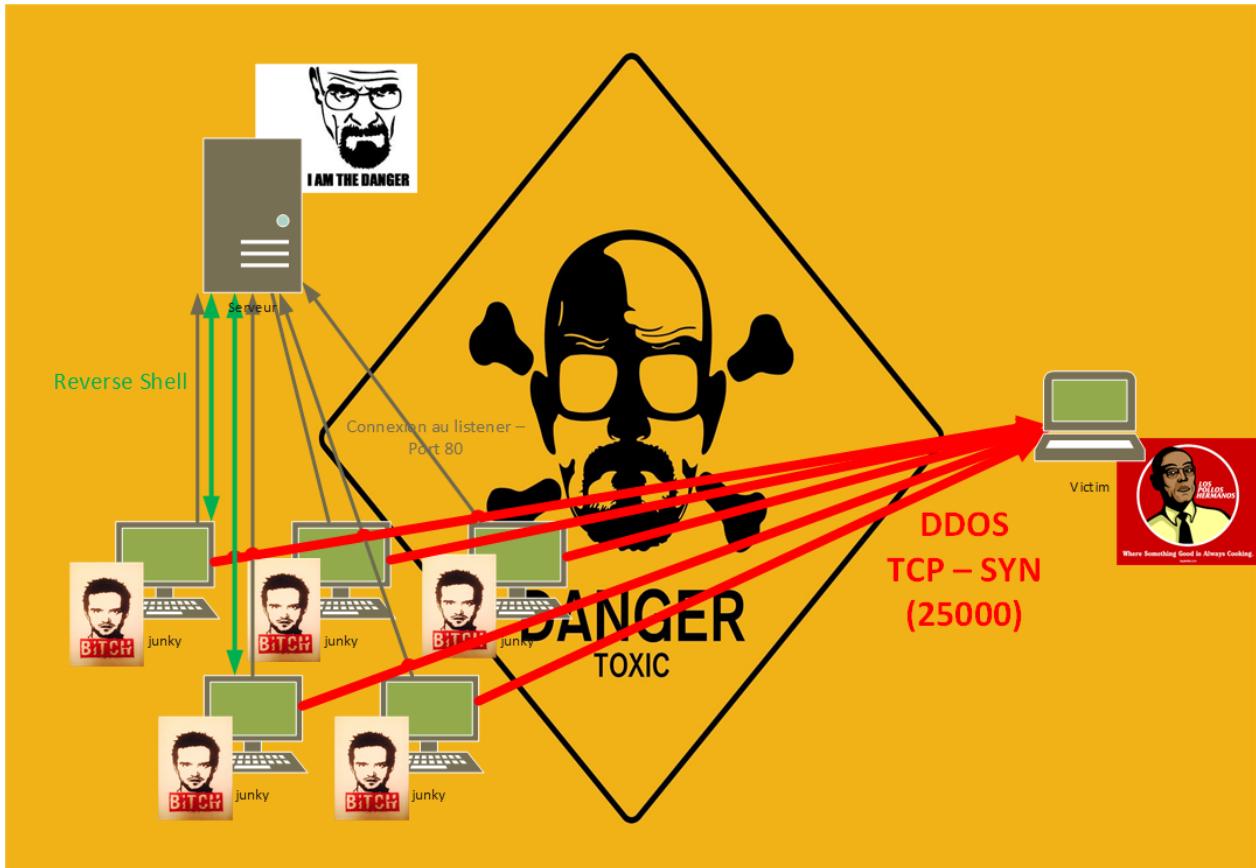


Shéma de l'analyse fonctionnelle





Shéma de la topologie





L'avancée journalière du projet avec Trello



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.

Le scénario ci-dessous:

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! Pour ne pas citer la série...Vince pour les intimes à décider d'annoncer la préparation du film BREAKING BAD qui sera basé sur l'histoire de WALTER WHITE, de son enfance à son ascension de criminel! 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 coeur de rédacteur et de fan.

L'affiche ICI





Réalisation d'un wrapper avec l'image du phishing