Charte-Projet

PPII2 - 2025

BELLEC – SORAGNA - FERNANDEZ DEL BUSTO JIMENEZ – ZANELLA

Sommaire

1 – Cadrage

A. Contexte

Dans le cadre du second semestre de notre première année de formation à l'école d'ingénieurs TELECOM Nancy, il nous a été demandé de travailler sur un projet pluridisciplinaire d'informatique intégrative. L'utilité pédagogique de ce projet réside dans le fait qu'il va nous permettre de mettre en pratique les connaissances que nous avons acquises à l'école en travaillant sur un projet concret en équipe. Nous allons devoir croiser plusieurs types de connaissances issues de différents modules de la formation (Langage C, Structures de données, Réseaux, Algorithmie, Gestion de projets, ...) et travailler en autonomie durant près de trois mois en vue de produire plusieurs livrables répondant à un cahier des charges.

B. Finalités

De notre côté, la finalité première de ce projet consiste en l'acquisition de nouvelles compétences et connaissances. Notre équipe devra par ailleurs produire plusieurs livrables d'ici au 26 mai 2025. Ces livrables seront étudiés puis évalués par nos enseignants. Le rendu des livrables sera suivi au début du mois de juin par une soutenance de groupe face à un jury composé de deux membres de l'équipe pédagogique.

La note obtenue à l'issue du projet sera comptabilisée dans le cadre de la validation de notre semestre et témoignera de notre investissement et de la qualité de nos productions.

C. Objectifs

Résumé du cahier des charges

L'objectif de ce projet est de concevoir un botnet composé d'un serveur « Command and Control » (C&C ou C2) « responsable de la coordination des bots et de l'envoi des instructions » et de multiples clients esclaves « qui s'enregistrent auprès du serveur C&C, exécutent des commandes reçues de ce serveur et lui envoient un rapport sur ces exécutions » en langage C. De plus, un outil d'interface permettant au bot-master (l'utilisateur contrôlant le serveur C&C et à fortiori les machines zombies du botnet) de contrôler le botnet.

Le périmètre du projet se limite néanmoins à la phase opérationnelle du botnet, on supposera que les bots s'exécutent avec les droits administrateurs sur leurs machines hôtes respectives. Les points suivants seront ainsi considérés comme en dehors du périmètre du projet :

- La phase d'expansion du botnet (identification et infection de nouvelles machines)
- La phase d'escalade de privilège du bot sur sa machine hôte nouvellement infectée.
- Le phase de dissimulation du bot sur sa machine hôte.

Ainsi, nous allons devoir développer plusieurs programmes en langage C capables de communiquer via le réseau en utilisant les sockets. L'un des programmes à développer sera un programme maître, capable de gérer plusieurs connexions simultanées et de faire

exécuter à plusieurs programmes esclaves des commandes précises sur leurs machines hôtes respectives. Les bots devront avertir le serveur C&C de leurs activités, tandis que celui-ci tiendra à jour un fichier de journalisation des bots connectés au réseau ainsi que des commandes qui leur ont été envoyées.

L'interface utilisateur devra, selon les spécifications fournies par nos enseignants, permettre de fournir à l'utilisateur la liste des bots actifs sur le réseau et de rendre possible le fait de choisir une commande à exécuter et de la transmettre à des bots spécifiques sur le réseau.

Voici une description du cahier des charges minimal attendu pour le serveur C&C :

- Capacité à gérer plusieurs clients via les sockets TCP.
- Envoi de commandes aux bots.
- Journalisation des bots connectés et des commandes exécutées sur le botnet.
- Ajout et suppression de bots au réseau.

Et voici une description du cahier des charges minimal attendu pour les bots :

- Récupération d'informations système.
- Simulation de trafic massif et coordonné sur une cible définie (Attaque DDoS).
- Simulation d'une attaque Flooding TCP/SYN vers une cible définie.

Nous sommes par ailleurs invités à compléter ces fonctionnalités par des tâches « spéciales » et des fonctionnalités optionnelles pour ces bots dont voici quelques exemples :

- Exécution de commandes systèmes.
- Téléchargement vers les bots de fichiers binaire à exécuter.
- Chiffrement de fichiers sur les machines hébergeant les bots.
- Chiffrement des communications entre le serveur C&C et les bots.
- Système de mise à jour des bots par le C&C.
- Optimisation de la discrétion des communications sur le botnet.

La nature de ces attaques exige de nous plusieurs précautions importantes dont nous allons souligner l'importance plus tard dans ce document.

Technologies

Afin de mener à bien ce projet, nous allons utiliser exclusivement le langage C afin d'implémenter le serveur C&C et les scripts « zombies ». Naturellement, l'utilisation de bibliothèques spécialisées (par exemple concernant les sockets) seront utilisées et des structures de données spécifiques seront implémentées par notre équipe.

En ce qui concerne la partie relative au développement de l'interface d'administration du botnet, nous utiliserons le langage C et peut être Bash afin de proposer un menu en ligne de commande à l'utilisateur.

Échéances et liste des livrables

Il nous a été indiqué que les livrables consisteront « à minima » en :

- Le code source du projet et une liste d'instructions afin de l'exécuter.
- Un état de l’art sur le fonctionnement général des botnets.
- Une documentation du projet et de ses détails techniques comprenant nos documents de gestion de projets et de conception.
- Plusieurs tests unitaires relatifs au code source.

Ces livrables devront être rendus via le dépôt GitLab du projet au plus tard le Lundi 26 mai 2025. Une soutenance orale viendra compléter ce rendu au début du mois de juin 2025. Cette soutenance sera l’occasion de présenter une démonstration de notre projet puis d’échanger avec un jury composé de deux membres de l’équipe pédagogique de TELECOM Nancy.

2 – Déroulement du projet

A. Organisation

Nous utiliserons une méthode de gestion de projet agile. Nous allons découper le travail à accomplir en sous objectifs auxquels nous allons attribuer une « deadline » afin de respecter le calendrier de rendu. Ces tâches seront réalisées lors de sprints.

Pour cela, nous utilisons plusieurs outils, parmi lesquels :

- L'outil de gestion de versions GitLab, de manière à gérer la collaboration entre les membres de notre équipe au niveau du développement des fonctionnalités du projet.

- La messagerie Discord, dans l'optique de rendre la communication la plus simple et rapide possible entre les membres de l'équipe.

- Youtrack, un outil de gestion de projet développé par JetBrains et aux fonctionnalités nombreuses.

YouTrack sera le point central de notre gestion de projet, cet outil permet en effet de créer et de maintenir à jour des boards agiles et de définir des sprints. Cet outil permet aussi de centraliser de l'information, par exemple des documents de gestion de projet ou de la documentation technique.

Ceci nous permettra d'avoir un très bon visuel global sur les tâches à accomplir ainsi que sur les tâches affiliées aux sprints agiles en cours. Notre réactivité et notre capacité à affecter nos forces sur différents points du projet s'en trouveront accrues. L'adoption d'une méthode de travail agile dans le cadre de ce projet est rendue possible par une absence de gestion de budget ainsi que par la taille réduite de notre équipe.

B. Précautions d'usage

Les expériences qui seront menées par notre équipe lors des phases de test des fonctionnalités de Ddos et de Flooding TCP relatives aux bots devront être menées dans un environnement réseau contrôlé et isolé. La nature illégale de ces attaques implique qu'il est formellement interdit de tester ces fonctionnalités sur un réseau réel, quel qu'il soit.

Afin de respecter ces points, nous sommes invités à mener nos tests dans des environnements isolés de type Docker ou machines virtuelles locales. En outre, l'équipe pédagogique de TELECOM Nancy se tient disponible en cas de questions ou de requêtes de notre part en lien avec ces questions relatives à la sécurité des réseaux et aux précautions d'usage.

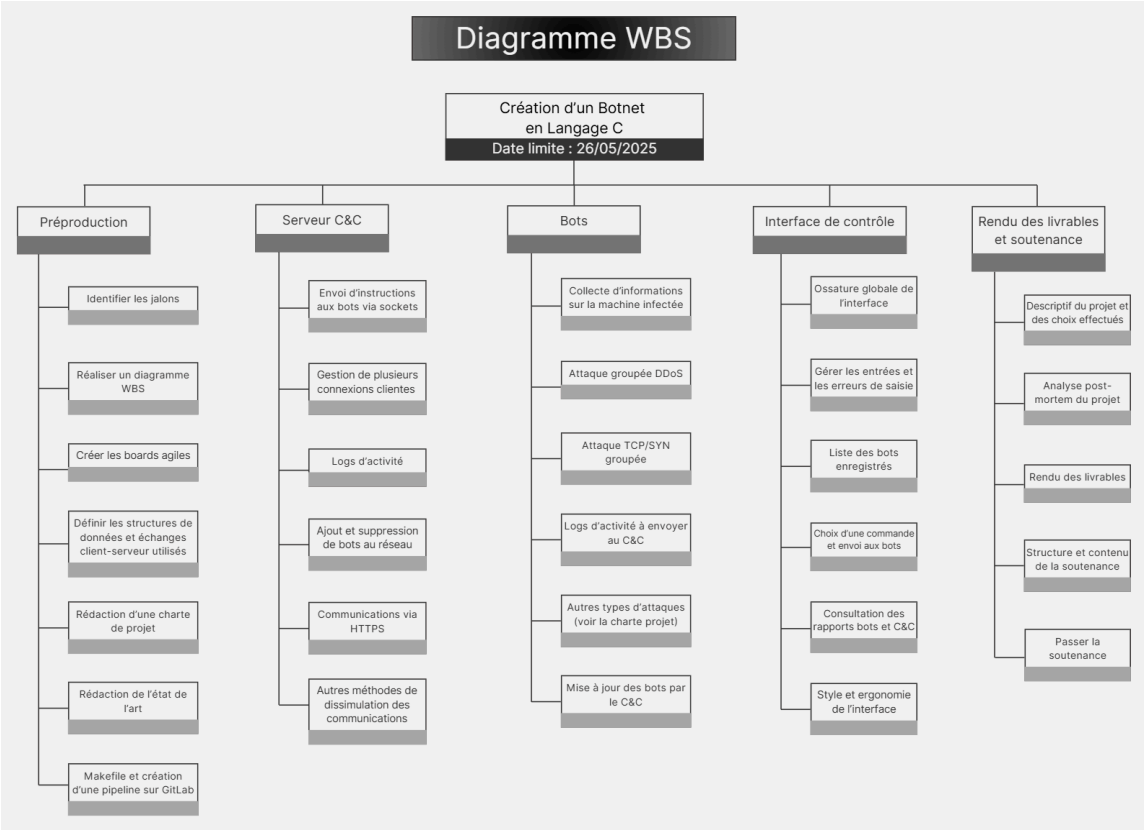
C. Jalons

Description de la méthode de découpage

Comme précisé dans la partie précédente, nous avons découpé le projet en sous-tâches en vue de respecter le calendrier de rendu global. Pour ce faire, nous avons suivi la méthode de découpage WBS (Work breakdown structure) visant à découper un projet en lots de travail puis en sous lots unitaires.

Diagramme WBS

Vous trouverez ci-dessous le diagramme WBS du projet.



Le découpage s'effectue selon une logique structurelle : chaque tâche est décomposée en sous-tâches la constituant.

La lecture du document s'effectue de gauche à droite, une notion d'ordonnancement des tâches est observable bien qu'il nous sera toujours possible d'être flexibles et de travailler sur des tâches différentes simultanément.