2024

Rapport écrit - Projet Fil Rouge - Labo Cybersécurité

DUCRET Jules

Ynov Bordeaux Campus

12/05/2024

Sommaire :

Projet Fil Rouge - Approche sur le reverse Engineering

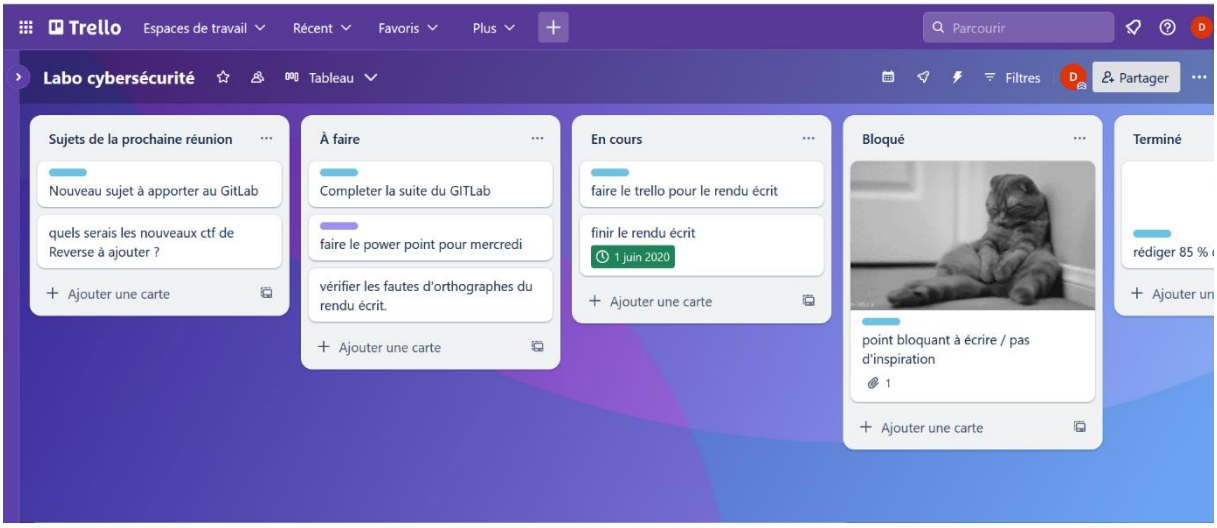
Ce rapport écrit apporte une vue d'ensemble sur ce projet établi le long de cette année 2023/2024 lors du « Ydays – Laboratoire Cybersécurité ». J'ai réalisé ce projet seul, où j'ai tenté de créer une approche sur le sujet du Reverse Engineering. Elle permet de comprendre le but et les failles d'un exécutable ou d'un code donné afin d'attendre un but précis. Cette partie de la Cybersécurité est utile en Blue Team comme en Red Team et apparaît dans certains CTF (Capture The Flag).

J'ai choisi ce sujet car c'est celui appartenant à la cybersécurité qui me plaît le plus et dans celui que je voulais apprendre durant ce Ydays. J'ai orienté ce projet sur la prise de connaissance accessible pour de futurs étudiants. Il est stocké sur un projet GitLab qui sera accessible en public. Il comporte des bases qui seront à parcourir en cas de besoin pour comprendre certains points évoqués dans les différentes méthodes de Reverse Engineering discutées au cours de la deuxième partie ainsi que les différents outils proposés au cours de la troisième. Ces méthodes pourront être pratiquées, testées sur différents exécutables disponibles sur le Gitlab.

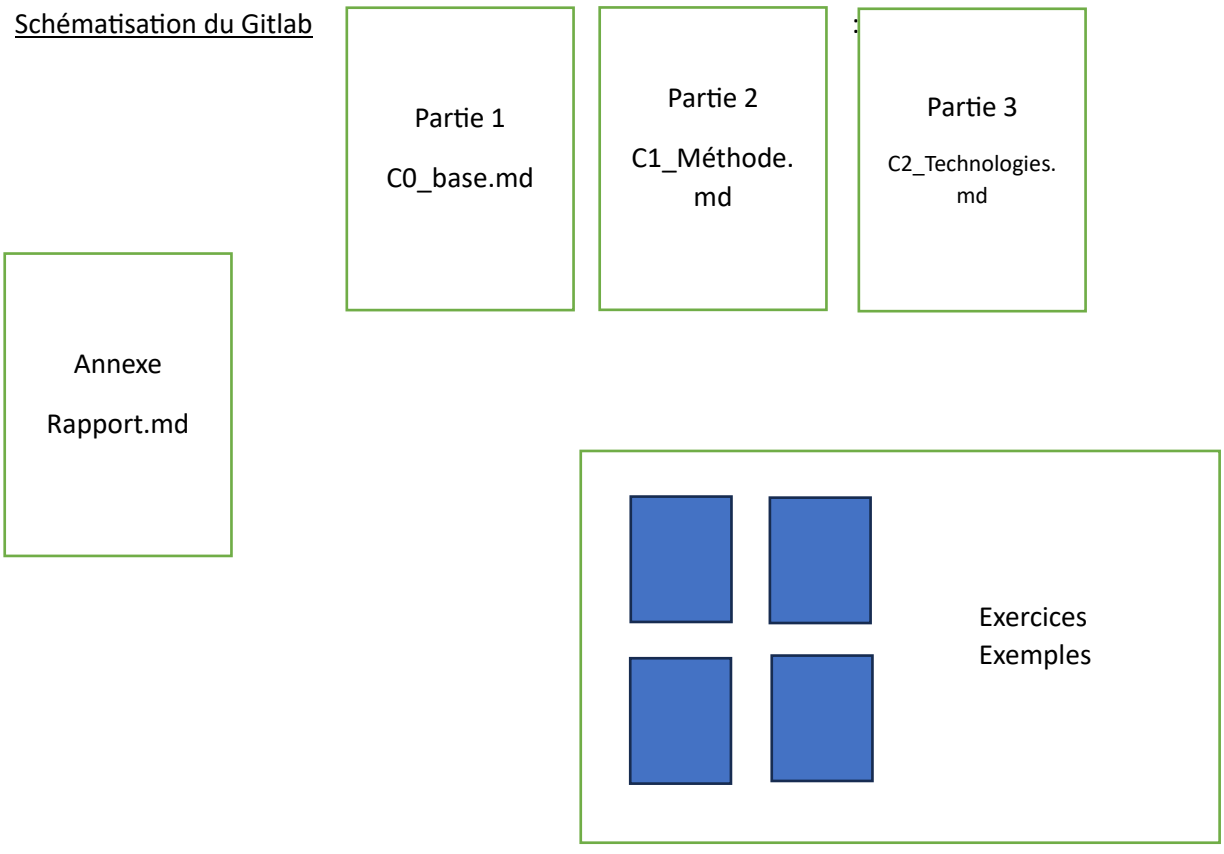
Description et Schématisation du projet :

Comme évoqué juste avant, le Marckdown se compose de plusieurs parties dont les bases, les méthodes, les outils. On pourra retrouver en plus de cela certains exécutables disponibles pour tester les méthodes évoquées. Chaque partie est accessible sur différents marckdowns pour faciliter la lecture. A la fin de chaque page, un lien est disponible pour la partie suivante, la précédente et l'annexe en générale.

J'ai organisé mon projet avec Trello afin de découper mes différentes tâches. En général, Trello est plus utile pour les travaux de groupe et la répartition de tâches entre différentes personnes appartenant au groupe mais peut aussi être utilisé en solitaire sur l'organisation des tâches effectuées et à venir.



Schématisation du Gitlab :



Historique du projet :

Pour cette partie des problématiques rencontrées, du fait que mon projet n'est pas technique, je n'aurais pas beaucoup de problématiques à montrer. Les problématiques techniques que j'ai rencontrées, ont été sur la construction d'exécutables pour permettre aux futurs utilisateurs de tester les solutions. Par exemple, trouver le bon code à implémenter afin de permettre une faille et de l'exploiter avec du Reverse Engineering. Pour corriger cela, j'ai cherché sur internet pour trouver les bonnes fonctions à implémenter. J'ai aussi cherché des solutions avec des CTF présents sur des plateformes comme Rootme.

J'ai aussi rencontré des difficultés à générer des idées pour aborder les différentes parties de mon Gitlab, pour résoudre ce genre de difficulté, j'ai essayé de voir les différents points abordés dans des livres qui parlent du sujet.

Conclusion :

Ce projet m'a permis au long de cette année 2023/2024 de compléter mes connaissances en Reverse Engineering, des connaissances sur de nouveaux outils toujours en rapport au Reverse Engineering. Ainsi que de compléter en partie ma veille technologique sur les différentes manières d'approcher un programme.

Je pense que le GitLab peut être complété avec d'autres notions plus avancées, et qu'il pourra l'être dans le futur lorsque de nouvelles techniques, failles, outils seront découverts. Cette partie est toujours indiquée dans le Trello comme point toujours en cours.

Annexes :

Lien du Gitlab :

https://gitlab.com/jujududu/raport-projet-cybersecu-lab

Lien du Trello :
https://trello.com/invite/b/gUH15GYn/ATTI8423e534319fcc9228e5e3e326414cef8F4E7CAD/labo-cybersecurite

Chaine YouTube :

https://www.youtube.com/@LiveOverflow

Mon Root-me:

https://www.root-me.org/Ganesh-651324

Rendu du laboratoire de cybersécurité	
Jules Ducret	A rendre pour le 12/05/2024
Groupe-9	Sujet : Notion d'apprentissage du Reverse Engineering