Préambule

Au cours de notre deuxième année de DUT en réseaux et télécommunications, nous avons réalisé un projet en groupe tutoré par M. GUILLEMIN ainsi que M. CHEVALLIER. Notre projet, qui a pour but d'augmenter notre autonomie et notre esprit de recherche face à une tâche complexe, a été orienté vers la sécurité informatique. En effet, notre sujet « Capture the flag » ou plus couramment appelé CTF, est un exercice d'infiltration système qui permet de vérifier la sécurité d'un service informatique. Le projet CTF a été mis en place en Septembre 2019. Nous n'avons donc reçu aucune base de nos aînés, ce qui va impliquer un rapport contenant majoritairement de la documentation à propos des outils d'infiltrations présent sur la distribution Kali Linux.
Sachant que le sujet est très vaste, nous allons essayer de nous focaliser sur des attaques de serveurs Web afin de pouvoir complètement traiter la question.

Avant de commencer à lire ce rapport, il est essentiel de savoir que tout ce qui y est répertorié ne doit en aucun cas être utilisé contre un système sans l'autorisation de son propriétaire au risque de lourdes peines.

Présentation du projet

Le CTF

La sécurité informatique au sein d'une entreprise est devenue le domaine avec le plus grand enjeux. Il faut donc du personnel spécialisé dans ce domaine afin de la mettre en place. On se rend facilement compte que le meilleur moyen de s'améliorer dans ce milieu est dans un premier temps de se documenter puis de réaliser des attaques. C'est à ce moment-là que le "Capture The Flag" ou bien "Capturer Le Drapeau" intervient. A l'origine, un CTF est un jeu à l'air libre où deux équipes s'affrontent pour s'emparer du drapeau de l'adversaire. On peut alors s'apercevoir que le monde informatique est semblable à celui réel. En effet, notre CTF a pour but d'infiltrer une machine cible et de trouver un document, le drapeau, en toute légalité. Le CTF s'est démocratisé en 1996 lors des premières compétitions organisées par la DEF CON. La DEF CON est la convention de hackeur la plus connue du monde.
Les CTF s'inspirent de la vraie vie même si cela reste un terrain d'entraînement. Les CTF reposent sur plusieurs domaines qui sont : le reverse engineering, l'exploitation web, le forensic, le réseau, la cryptographie, la sécurité mobile et la stéganographie. Tous ces domaines sont les piliers de la sécurité informatique. Il faudra donc être polyvalent afin d'exploiter les failles et de résoudre un CTF. Nous allons donc voir au cours de ce rapports différents moyens de parvenir à nos fins.

L'organisation du projet

A la suite du choix du projet et de la création du groupe pour ce dernier, il a fallu nous organiser afin que de communiquer de manière rapide et pratique. Nous avons donc créé un serveur Discord nous permettant de communiquer en temps réel. Discord est un logiciel gratuit de communication, réalisé pour la communauté du gaming, utilisable sur tout type de support moderne avec accès à internet. Cet utilitaire nous permet d'obtenir une banque de données, un chat vocal et textuel, le tout sur une seule application. Nous avons pu, grâce à ce support, travailler chez nous tout en travaillant ensemble. Pour ce qui est l'écriture du rapport, nous avons choisi de travailler sur Google Drive dans le but de ne jamais perdre notre travail et aussi de l'utiliser en même temps que d'autres membres du groupe.
Nous nous sommes réparti le travail et avons mis en place le diagramme de Gantt suivant afin de nous organiser :

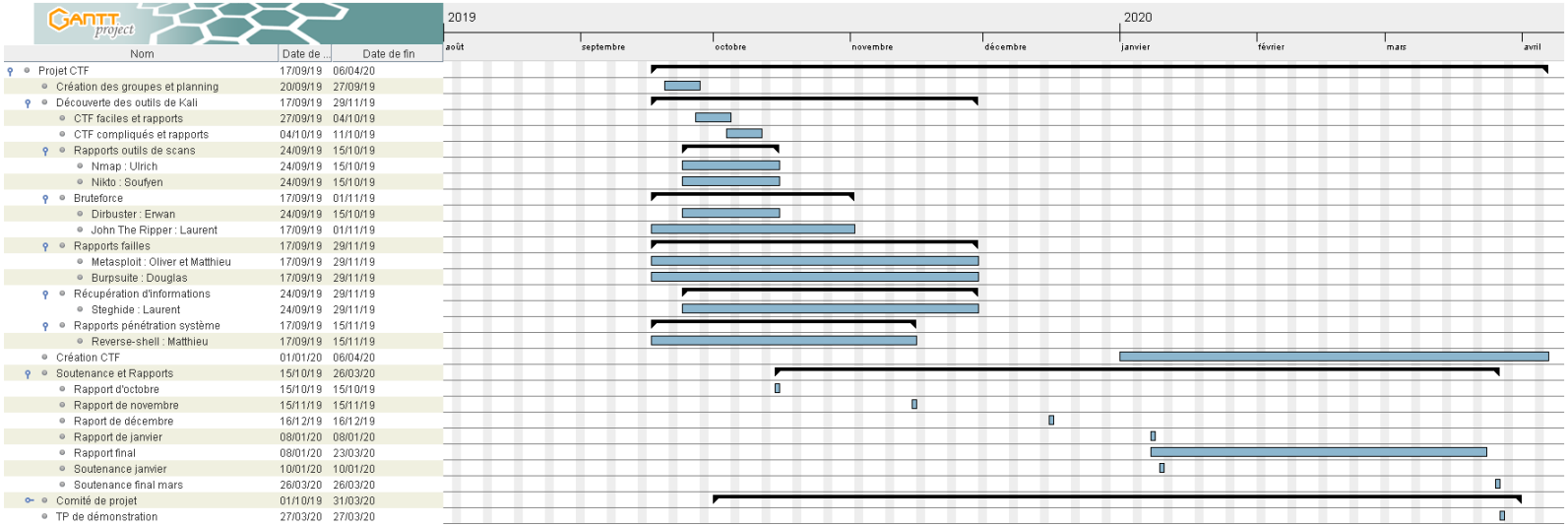

FIGURE 1 – Diagramme de Gantt