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

Objectif du projet

Le projet CTF a été découpé en trois axes sur un interval de six mois de travail. Ces trois axes sont :

— La documentation des outils sous Kali Linux
— Mise en place d'attaques sur des CTF
— Création d'un cours à partir du projet

Dans un premier temps, nous devions nous intéresser aux outils présents sur Kali Linux et les documenter. Dans cet axe, en plus de documenter, nous devions expliquer le fonctionnement de chaque outil. Ensuite, nous avons dû réaliser des CTFs afin d'utiliser les outils sur des cas pratiques. Ces attaques ont servi d'exemples dans la présentation des outils. Pour terminer, il nous a été demandé de transformer notre travail en un module de cours pour notre promotion et les suivantes.

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 de l'écriture du rapport, nous avons choisi de travailler sur Overleaf [1] 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 :

1. Overleaf est un éditeur web de Latex.

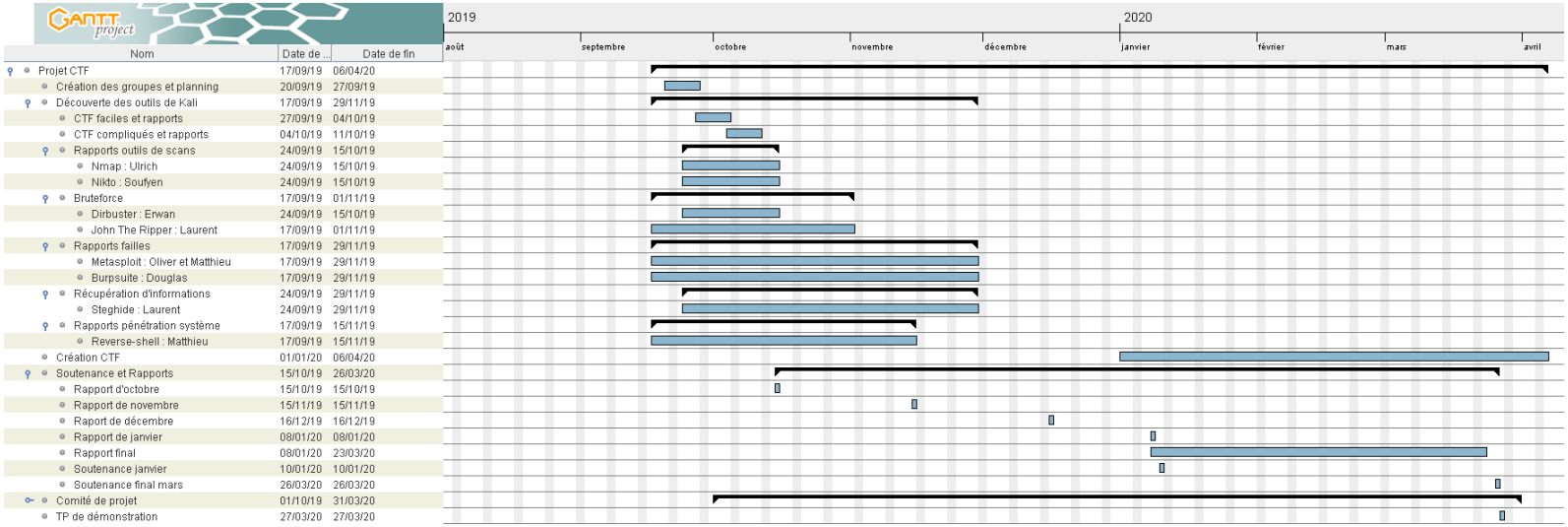

FIGURE 1 – Diagramme de Gantt

3

Comme vous pouvez le voir ci-dessus, nous nous sommes dans un premier temps répartis les outils à anlayser en nous donnant comme date butoire le 29 novembre 2019. Cet objectif a été dépassé ce qui nous a permis en Janvier 2020 de compléter la totalité des objectifs de ce diagramme. C'est pour cette raison qu'un troisième axe de création de module a été mis en place à partir de février 2020. Ce cours, qui comprend l'entièreté de notre travail, servira de rapport final du projet CTF 2019-2020.