Rapport du Projet CTF

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Encadré par :
M.Briffaut

Réalisé par :
Salma FDIL
Saida BAHRAOUI
Mariame OUBANI
Nhat Huy TRAN

2024-2025

Remerciements

*Nous tenons à exprimer notre profonde gratitude à **M. Briffaut**, notre encadrant, pour son soutien constant, sa patience et son expertise tout au long de ce projet. En tant que directeur du département **STI - Sécurité et Technologies Informatiques** à l'INSA Centre Val de Loire, ses conseils ont été précieux pour mener à bien notre projet. Nous lui adressons nos sincères remerciements pour sa disponibilité et sa bienveillance.*
Nous souhaitons également remercier tous les membres des autres groupes qui ont participé à ce projet. Leur collaboration a été essentielle dans la réussite de cette initiative, et nous leur sommes reconnaissants pour leurs idées, leurs efforts et leur esprit d'équipe.

Résumé du Projet CTF en français

Ce projet a pour objectif la création et la résolution de défis de cybersécurité sous forme de Capture The Flag (CTF), afin d'améliorer les compétences en sécurité informatique. Plusieurs scénarios de CTF ont été développés, couvrant des domaines tels que l'exploitation de vulnérabilités web, la cryptographie et l'analyse de trafic réseau. Les défis ont été hébergés sur GitHub et déployés sur OpenStack pour simuler des environnements sécurisés. Des vidéos explicatives ont été créées pour aider à la résolution des CTF. Après leur mise en ligne, une phase d'attaque a permis de résoudre des CTF provenant d'autres groupes. Ce rapport présente les étapes clés du projet et les résultats obtenus

Résumé du Projet CTF en Anglais

The objective of this project is to create and solve cybersecurity challenges in the form of Capture The Flag (CTF), aimed at improving skills in information security. Several CTF scenarios were developed, covering areas such as web vulnerability exploitation, cryptography, and network traffic analysis. The challenges were hosted on GitHub and deployed on OpenStack to simulate secure environments. Explanatory videos were created to assist in solving the CTFs. After deployment, an attack phase allowed us to solve CTFs from other groups. This report presents the key steps of the project and the results obtained.

Sommaire

1- Introduction

La cybersécurité représente un enjeu majeur dans le monde numérique actuel. Pour renforcer les compétences en sécurité offensive et défensive, notre projet propose la création de plusieurs types de **Capture The Flag (CTF)**, permettant aux participants de tester et d'améliorer leurs connaissances dans des domaines variés.

Ces défis interactifs se concentrent sur l'exploitation de vulnérabilités web, la cryptographie, et l'analyse de trafic réseau.
L'objectif est de concevoir un environnement de jeu sécurisé, basé sur des vulnérabilités réalistes, où les joueurs devront exploiter des failles pour récupérer des "flags".

Le projet sera déployé sur **OpenStack**, avec l'utilisation d'instances pour le développement et l'analyse des défis. De plus, l'intégration de **Docker** facilitera la mise en place d'un environnement isolé et reproductible, garantissant une expérience cohérente pour tous les participants.

2.Définitions des concepts clés

2.1. CTF (Capture The Flag)

2.1.1.Définitions

Un Capture The Flag (CTF) est une compétition dans laquelle les participants doivent résoudre des défis dans différents domaines de la cybersécurité pour récupérer des "flags", des chaînes de caractères qui prouvent que la solution a été trouvée. Chaque CTF teste les compétences des participants dans des situations réalistes. Ces compétitions couvrent plusieurs domaines, notamment l'exploitation de vulnérabilités logicielles, l'analyse de trafic réseau, la cryptographie, l'analyse de systèmes, et bien plus encore.

2.1.2. Types de CTF

Les types de CTF sur lesquels nous avons travaillé dans notre projet :

CTF Réseau :

Les CTF Réseau se concentrent sur l'analyse et l'exploitation de réseaux. Les participants doivent intercepter, analyser, ou manipuler du trafic réseau pour obtenir des informations sensibles. Ces défis peuvent inclure des tâches telles que la capture de paquets réseau (par exemple avec Wireshark), l'analyse de protocoles réseau ou encore la mise en place d'attaques de type Man-in-the-Middle (MITM). L'objectif est d'exploiter les vulnérabilités présentes dans les communications réseau pour extraire des flags.

CTF Web :

Les CTF Web portent sur l'exploitation de vulnérabilités dans des applications web. Cela peut inclure des attaques telles que l'injection SQL, les failles XSS (Cross-Site Scripting), ou l'exploitation de mauvaises configurations des serveurs web. Les participants sont amenés à explorer des sites web vulnérables, à analyser les paramètres d'URL, et à manipuler les formulaires pour accéder à des informations sensibles ou injecter des commandes.

CTF Osint :

Les CTF Osint se concentrent sur la collecte d'informations à partir de sources publiques (open source). Cela inclut la recherche d'informations sur Internet, l'extraction de données provenant de réseaux sociaux, de sites web publics, ou de bases de données accessibles en ligne. Les participants doivent utiliser des outils d'analyse d'OSINT, comme les moteurs de recherche avancés ou des scripts pour récupérer des informations cachées qui les aideront à résoudre le défi.

CTF Cryptographie :

Les CTF Crypto sont des défis qui mettent à l'épreuve les compétences des participants en cryptographie. Cela peut inclure le décryptage de messages chiffrés, la résolution de puzzles cryptographiques complexes, ou l'utilisation de failles dans les algorithmes de chiffrement. Ces défis peuvent couvrir une large gamme de techniques cryptographiques, comme les chiffres de César, le chiffrement RSA, ou encore les attaques par force brute.

CTF Système :

Les CTF Système se concentrent sur l'exploitation de failles au niveau des systèmes d'exploitation. Cela inclut des attaques comme l'exploitation de failles de sécurité dans le noyau, la manipulation des permissions des fichiers, ou la recherche de vulnérabilités dans les programmes qui tournent sur un système cible. Ces défis sont souvent plus complexes et nécessitent une connaissance approfondie des systèmes d'exploitation, de la gestion des utilisateurs, et des techniques d'escalade de privilèges.

2.1.3. Les Étapes Fondamentales d'un CTF

Un CTF classique se décompose généralement en plusieurs phases :

Scanning :

Dans cette première étape, les participants commencent souvent avec l’adresse IP de la machine cible. Ils effectuent un scan pour découvrir les ports ouverts, ce qui permet de déterminer les points d’entrée potentiels pour l’attaque à venir. Le scanning peut aussi révéler des informations supplémentaires comme le système d’exploitation utilisé et les services en cours d'exécution sur la machine cible.

Enumération :

Une fois les informations de base obtenues par le scanning, l’étape d'énumération consiste à approfondir la recherche d’informations spécifiques à exploiter. Cela inclut la recherche de serveurs web, de services FTP, de pages cachées, de points d'entrée sur des systèmes, et plus encore. Cette phase est cruciale pour réussir un CTF, car elle fournit des indices sur comment pénétrer dans la machine cible.

Exploitation :

L’exploitation est l’étape où la stratégie pour pénétrer dans la machine cible est mise en action. En fonction des informations collectées lors de l'énumération, les participants essaient de se connecter à la machine cible, en exploitant les vulnérabilités trouvées. Cette phase mobilise des connaissances diverses, incluant la cryptographie, l’analyse de paquets réseau, l’analyse de code binaire, le reverse engineering, la stéganographie, et la cybersécurité en général.

Escalade de privilèges :

Une fois que l'accès à la machine cible est établi avec un compte utilisateur de base, il reste à obtenir un accès complet (Root). L'escalade de privilèges consiste à exploiter des failles dans le système pour obtenir un contrôle administratif, ou root. Dans les CTF les plus simples, l'accès root peut être atteint rapidement, tandis que dans les plus complexes, plusieurs étapes d'escalade peuvent être nécessaires.

2.2. OpenStack

OpenStack est une plateforme open-source dédiée à la gestion de cloud computing. Elle permet de créer, déployer et gérer des infrastructures cloud privées ou publiques. OpenStack offre une large gamme de services pour la gestion de machines virtuelles, de réseaux, de stockage et d'autres ressources essentielles dans un environnement cloud.

Dans le cadre de ce projet, OpenStack a été utilisé pour héberger les défis CTF dans des environnements virtuels sécurisés. Nous avons créé plusieurs instances virtuelles sur OpenStack, permettant ainsi de déployer nos CTF dans des environnements isolés et contrôlés. Cela a offert aux participants un cadre sécurisé pour interagir avec les défis, tout en s'assurant qu'ils sont exécutés dans des conditions réalistes et sans risque pour les systèmes extérieurs.

L'utilisation d'OpenStack a joué un rôle clé dans le projet en garantissant une infrastructure flexible et scalable, adaptée aux besoins variés des différents défis CTF. Les instances ont été configurées pour simuler différents scénarios d'attaque, rendant chaque défi accessible et immersif pour les participants.

2.3. GitHub

GitHub est une plateforme de développement collaboratif qui repose sur Git, un système de gestion de version. Elle permet aux utilisateurs de stocker, partager et collaborer sur des projets de code, tout en facilitant le suivi de l’évolution de ces projets. GitHub est couramment utilisée par les développeurs pour gérer les versions de leurs projets et travailler de manière collaborative avec d'autres personnes.

Dans le cadre de ce projet, GitHub a été utilisé pour plusieurs fonctions essentielles. Les scénarios de CTF, les vidéos explicatives intitulées "Video-Solution", ainsi que la documentation associée ont été hébergés sur notre dépôt GitHub. Cela a facilité l'accès à ces ressources pour les participants et a permis un partage facile entre les membres de l'équipe et les participants externes.
De plus, GitHub a joué un rôle central dans la gestion des images Docker utilisées pour nos CTF. Les Dockerfiles et les images Docker nécessaires à la mise en place des environnements CTF ont été stockés dans le dépôt, permettant aux participants de déployer rapidement les environnements isolés et reproductibles. Cette utilisation de Docker a facilité la mise en place d'environments de challenge sécurisés et standardisés, tout en garantissant leur portabilité.

3.Étapes du projet

3.1. Création des CTFs

Dans le cadre de ce projet, plusieurs défis CTF ont été créés et hébergés sur OpenStack pour offrir une diversité d'expériences aux participants. Ces CTFs couvrent différentes thématiques de la cybersécurité, allant du Web, de l'OSINT, du Réseau, du Système jusqu'à la Cryptographie, avec des niveaux de difficulté variés (facile, moyen et difficile).

Niveau Facile

Web – SQL Injection :

- Description : La base de données du site contient un tableau "users" avec des informations sur chaque utilisateur. L'un d'eux, nommé "briffaut", détient le flag.
- Objectif : Utiliser des techniques de SQL Injection pour extraire le flag stocké dans la base de données.

OSINT – Profil d'entreprise

- Description : Un faux compte Facebook d'une entreprise a été créé, contenant plusieurs employés fictifs. Parmi eux, un employé passionné de voyages laisse des indices précieux pour retrouver le flag.
- Objectif : Effectuer une enquête OSINT en analysant les profils et indices dissimulés.

Réseau – Maître en Wireshark

- Description : Une employée a utilisé un protocole non sécurisé, entraînant la capture de ses credentials et activités réseau via Wireshark.
- Objectif : Analyser le fichier .pcapng pour identifier et extraire le flag.

Système – Escalade de privilèges

- Description : Le participant doit se connecter à une VM avec l'utilisateur "user". Un fichier admin_credentials.txt contient les identifiants pour un autre utilisateur "admin", qui permet d'accéder à un fichier caché : ./.hidden_folder/.flag_secret.
- Objectif : Escalader les privilèges et retrouver le flag.

Cryptographie – Les Secrets Cachés dans le HTML

- Description : Un fichier HTML contient un code binaire et une clé cachée. L'application d'un chiffrement XOR révèle un second code binaire.
- Objectif : Décrypter le message pour obtenir le flag.

Niveau Moyen

Web – Exploration et Obfuscation

- Description : Le participant doit retrouver des identifiants cachés dans index.html et script_obf.js, puis les utiliser pour accéder à une page secrète flag.html contenant le flag.
- Objectif : Manipuler l'encodage Base64 et Hexadécimal pour reconstituer les identifiants d'accès.

OSINT – Investigation et Décodage

- Description : Un défi plus complexe d'OSINT où les joueurs doivent analyser des métadonnées, décrypter des formats de données encodés et assembler des indices trouvés sur Facebook et GitHub.
- Objectif : Retrouver un flag divisé en deux parties.

Réseau – Analyse Wireshark avancée

- Description : Similaire au défi de niveau facile, mais les participants doivent analyser un protocole plus complexe pour extraire des informations cachées.
- Objectif : Détecter et extraire le flag du fichier .pcapng.

Système – Crontab et Obfuscation

- Description : Un crontab doit être exécuté deux fois pour obtenir le flag. Cependant, tous les fichiers de configuration sont chiffrés et obfusqués.
- Objectif : Déchiffrer et désobfusquer les fichiers pour exécuter le crontab avec succès.

Cryptographie – Déchiffrement et Brute-force

- Description : Un cryptologue de l'INSA a inventé un nouveau chiffrement et l'a utilisé pour crypter un message important.
- Objectif :
  - Briser l'algorithme de chiffrement,
  - Utiliser du brute-force pour retrouver les paramètres nécessaires,
  - Employer des scripts Python pour automatiser l'analyse et extraire le flag.

Niveau Difficile

Site caché de l'INSA

- Description : Le site officiel de l'INSA Centre Val de Loire est accessible via https://www.insa-centrevaldeloire.fr/. Cependant, un second site secret a été découvert à l'adresse http://176.129.192.118:1001. Ce site pourrait contenir des données intéressantes à exploiter.
- Objectif : Explorer et exploiter les failles du site pour en extraire le flag.

Remarque : Contrairement aux autres CTFs, ce défi n'a pas été hébergé sur OpenStack, en raison de manque d'espace sur openstack

3.2. Hébergement sur OpenStack

L’hébergement des CTFs sur OpenStack a nécessité plusieurs étapes techniques pour assurer leur accessibilité et leur bon fonctionnement. OpenStack a été utilisé pour déployer des machines virtuelles et les configurer afin d’accueillir nos défis de cybersécurité.

1. Connexion au VPN :

Avant toute interaction avec OpenStack, une connexion sécurisée au VPN de l’école était nécessaire. Cette étape permettait d’accéder à l’infrastructure et d’interagir avec les machines virtuelles. Cependant, nous avons rencontré des problèmes de connexion VPN avec le réseau de l’école, ce qui a parfois compliqué le déploiement des CTFs.

2. Création des Instances :

Une fois connectés au VPN, nous avons procédé à la création des instances sous OpenStack :

- Choix des configurations : Sélection des ressources (CPU, RAM, stockage).
- Installation des systèmes : Déploiement des systèmes d’exploitation selon les besoins des défis.
- Attribution des adresses IP : Configuration des adresses IP flottantes pour permettre l’accès aux machines.

3. Connexion aux Instances :

Après la création des instances, nous avons dû nous connecter aux machines pour installer et configurer les services nécessaires :

- Connexion via SSH avec une clé privée.
- Installation des services web, bases de données et outils de sécurité pour nos défis.
- Gestion des permissions pour éviter les erreurs d’accès.

Nous avons rencontré un problème de permissions SSH, où la connexion aux instances affichait "Permission Denied". Ce problème a été résolu en modifiant les permissions de la clé SSH avec chmod 600.

4. Hébergement des CTFs :

Une fois les machines configurées, nous avons hébergé les différents CTFs en fonction de leur nature :

- CTFs Web : Déploiement de serveurs web avec les fichiers des défis.
- CTFs Réseau : Mise en place d'environnements capturant du trafic réseau (fichiers .pcapng).
- CTFs Système : Configuration d'environnements nécessitant une escalade de privilèges.
- CTFs Cryptographie & OSINT : Stockage des indices et chiffrement des informations à décrypter.

Problème rencontré : Après le déploiement de la majorité des CTFs, nous avons constaté un manque d'espace de stockage, bien que nous ayons utilisé le minimum de ressources nécessaires pour chaque machine. Ce problème a nécessité un ajustement des ressources et une meilleure optimisation du stockage.

3.3. Phase d'attaque et identification des CTFs des autres groupes

Dans cette phase, nous avons analysé et attaqué les CTFs conçus par les autres groupes afin d'identifier leurs flags. Pour cela, nous avons appliqué différentes techniques adaptées aux types de défis rencontrés, notamment en web, OSINT, réseau, système et cryptographie. Nous avons utilisé divers outils et méthodologies, allant du scanning et de l'énumération à l'exploitation de vulnérabilités et au déchiffrement de données.

Grâce à ces approches, nous avons pu résoudre plusieurs CTFs et récupérer les flags correspondants. Voici les résultats obtenus pour **les autres groupes** :

Pour Groupe 3 :

Système Moyen

Nous avons réussi à identifier le flag de ce CTF en explorant un dossier accessible via SFTP, où trois fichiers étaient disponibles. Après les avoir téléchargés et analysés, nous avons utilisé Hydra pour effectuer une attaque par force brute et obtenir les identifiants nécessaires. En examinant le fichier cron-script.sh, nous avons constaté qu'il contenait un script conçu pour exécuter un reverse shell. Nous avons ensuite vérifié l'état du service Cron, modifié les permissions des fichiers et identifié un fichier caché qui nous a permis d'accéder au flag.

Les outils utilisés pour cette attaque incluent **SFTP** pour le transfert de fichiers, **Hydra** pour le brute-force des identifiants, **ls -la** pour la découverte des fichiers cachés, et cat pour l'affichage du contenu du script.

OSINT Moyen

Nous avons réussi à identifier le flag de ce CTF en accédant à une plateforme où plusieurs indices étaient dissimulés. Après avoir analysé les informations trouvées, nous avons utilisé CyberChef pour effectuer un double déchiffrement, d'abord en Base64, puis en ROT13, ce qui nous a permis d'extraire le flag.

OSINT facile

Pour ce ctf on commence à accéder au plateforme donnée par le groupe où on va trouver plusieurs comptes d'utilisateurs et chaque compte contient une photo on telecharge les photos et on essaye de l'analyser et ensuite on trouve le flag dans l'une des photos

Web facile

Après avoir utilisé la commande ffuf, nous avons trouvé la page web /robots.txt, qui contient deux autres pages. Dans la première, read.php, nous avons trouvé le premier flag. Ensuite, nous avons trouvé le deuxième flag en utilisant curl sur la deuxième page détectée, admin.php.

Système facile

Dans ce challenge, nous devions trouver les bons identifiants. Pour ce faire, nous avons utilisé FTP pour obtenir le nom d'utilisateur, puis Crunch et Hydra pour trouver le mot de passe. Après la connexion, afin d'accéder au fichier flag.txt, nous avons modifié les droits pour obtenir les privilèges root. Enfin, après ce changement de droits, nous avons trouvé le fichier souhaité contenant le flag.

Réseau facile

Nous avons trouvé la liste username.txt et password.txt et l'avons utilisée pour entrer en force dans le système. Après être entré dans le système, nous avons trouvé le flag sous forme codée en base64. décryptons-le et nous trouvons le flag

Cryptographie moyen

Peut-être à cause du problème du groupe 3, nous pouvons facilement lire le flag sans rien faire

Pour Groupe 1:

Facile cryptographie

Nous trouvons le flag en trouvant la clé id_rsa, puis en l'utilisant pour accéder au système et trouver le texte chiffré du flag. utilisez enfin un outil en ligne pour trouver le texte brut du flag

Moyen Cryptographie

Utilisez Wireshark pour lire les fichiers pcap et trouver les paramètres de l'algorithme Diffie-Hellman. j'ai finalement trouvé la clé et j'ai obtenu le flag.

Web facile

Voir le code source pour des conseils. utilisez l'outil burpsuite pour modifier la demande et nous trouvons flag

Web moyen

Voir le code source pour des conseils. Nous avons trouvé le fichier index.php situé dans le folder2. dans le système, nous trouvons le chemin vers le fichier index.php et trouvons le drapeau dans ce chemin

Système moyen

Nous avons trouvé un programme appelé ctf.py. Il s'agit d'un sandbox en python. Nous avons essayé d'utiliser « import os; os.system("/bin/bash") » et l'avons contourné avec succès et sommes devenus root. et nous lisons le fichier contenant le flag.

OSINT Moyen

En analysant les amis du compte trouvé dans osint facile on trouve un autre profile qui semble suspect et en cherchant on trouve beaucoup d’indices et une photo et après analyse de la photo on trouve le flag

Osint facile

En utilisant une chaîne de caractères déjà donnée et qui est chiffré on trouve que c’est un nom d’utilisateur donc on essaye de trouver le compte associé et on cherche dans ce compte où nous allons trouver le flag

System facile

Nous avons trouvé le flag en nous connectant en tant qu’admin avec les identifiants obtenus grâce à Hydra. Après la connexion, nous avons trouvé dans un fichier nommé file1 une chaîne de caractères que nous avons ensuite utilisée pour déchiffrer un fichier avec GPG.

3.4. Documentation des solutions

Pour résoudre les défis CTF des autres groupes, nous avons utilisé plusieurs outils spécialisés adaptés à chaque type de challenge :

- Web : Utilisation d'outils comme Burp Suite, SQLmap et Postman pour tester les vulnérabilités web (injections SQL, failles XSS, analyse des requêtes HTTP).
- OSINT : Recherche d'informations via Google Dorking, Maltego, l'analyse de métadonnées d'images et l'exploitation de profils sur les réseaux sociaux.
- Réseau : Utilisation de Wireshark pour analyser le trafic réseau, déchiffrer les communications et extraire des identifiants ou flags cachés dans les fichiers .pcapng.
- Système : Escalade de privilèges et analyse des permissions via Linux (sudo, cronjobs), récupération de fichiers cachés et reverse engineering sur des programmes.
- Cryptographie : Déchiffrement de textes avec CyberChef, utilisation de Python pour le brute-force de chiffrements, et exploitation de chiffrements XOR ou Base64.

Après avoir trouvé les solutions aux CTFs d'autres groupes, nous avons documenté ces solutions dans un fichier dédié sur GitHub. Ce fichier contient :

- Les solutions détaillées des CTFs des groupes 1 et 3.
- Les étapes et outils utilisés pour chaque challenge.

Cette documentation permet non seulement de conserver une trace de nos méthodologies, mais aussi de faciliter le partage de connaissances et d'améliorer les stratégies de résolution pour les futurs CTFs.

3.5. Problèmes rencontrés et solutions appliquées

1. ***Problème de connexion VPN***

   Lors de l'utilisation de la connexion VPN de l'école, nous avons fréquemment rencontré des problèmes de connexion, ce qui a entravé la fluidité du projet. Cela a nécessité des ajustements constants et une gestion des interruptions pour continuer les travaux à distance.

2. ***Problème de stockage***

   Après avoir déployé la majorité des CTFs sur nos instances, nous avons constaté que l'espace de stockage devenait insuffisant. Malgré l'utilisation d'un minimum de ressources pour chaque machine virtuelle, l'espace de stockage disponible n'a pas été suffisant pour gérer l'ensemble des défis déployés. Cela a exigé une optimisation de la gestion des ressources et un suivi des capacités de stockage.

Problèmes résolus :

1. ***Problème de permission avec la clé SSH***

   Lors de l'accès à nos instances pour modifier ou mettre à jour les défis, un message d'erreur "permission denied" apparaissait. Ce problème a été résolu en modifiant les permissions des fichiers via la commande chmod, ce qui a permis d'octroyer les droits d'accès nécessaires pour effectuer les modifications souhaitées.

2. ***Problème de MITM (Man-in-the-Middle) lors de connexions répétées***

   Lors de connexions répétées à nos instances, nous avons rencontré des problèmes liés à des attaques **Man-in-the-Middle (MITM)**, ce qui perturbait l'établissement de la connexion SSH. Ce problème a été corrigé en modifiant le fichier de configuration SSH, afin d'éviter l'interception des données et de sécuriser la connexion.

4.Conclusion

Ce projet de Capture The Flag (CTF) a été une initiative enrichissante et stimulante pour sensibiliser et former aux enjeux de la cybersécurité. À travers la création, l'hébergement et la résolution de défis, nous avons non seulement appliqué des concepts théoriques, mais aussi développé des compétences pratiques dans des domaines clés de la cybersécurité. L'utilisation de technologies telles que Docker, VPN et OpenStack nous a permis de créer un environnement virtuel sécurisé et d'explorer différents aspects de la sécurité informatique de manière réaliste.

Le projet nous a offert l'opportunité d'approfondir des notions techniques que nous avions étudiées, telles que la connexion SSH avec des clés, ainsi que d'acquérir des compétences dans des domaines variés comme l'analyse réseau, la sécurité web, et la cryptographie. L'intégration de défis en réseau, web et OSINT nous a permis d'expérimenter la résolution de problèmes complexes dans des situations proches de celles rencontrées par des professionnels de la cybersécurité.

Cependant, malgré les réussites et l'acquisition de nouvelles compétences, des difficultés ont été rencontrées, notamment dans la mise en place des environnements virtuels et la gestion des défis complexes. Ces obstacles ont constitué des opportunités pour identifier nos points faibles et nous ont permis de nous améliorer tout au long du projet.

En somme, ce projet CTF a été une expérience d'apprentissage précieuse, non seulement pour renforcer nos compétences techniques, mais aussi pour nous préparer à de futures missions en cybersécurité, tout en nous offrant une vision claire des défis et des opportunités dans ce domaine en constante évolution.

5.Annexes

5.1. Fichiers GitHub

« Documents-de-chaque-CTF » : Ce fichier sur GitHub contient tous les scénarios ainsi que les solutions de chaque CTF que nous avons créés. Chaque défi est détaillé avec les instructions nécessaires pour le résoudre, ainsi que les étapes et les techniques à utiliser pour trouver les flags.

« Solution CTF 1-3 »: Ce fichier contient les solutions des CTF que nous avons résolus pour les deux groupes. Il s'agit d'une compilation des résultats des défis de ces groupes, fournissant des réponses et des explications détaillées pour chaque problème abordé.

« Dockerfiles »: Chaque CTF créé est accompagné d'un Dockerfile correspondant. Ces Dockerfiles permettent de déployer un environnement isolé et reproductible pour chaque défi, en assurant une installation facile des outils nécessaires et une gestion cohérente de l'environnement d'exécution.

« Présentation du projet »: Un document contenant la présentation complète de notre projet, incluant la description des objectifs, des méthodologies employées, et des résultats obtenus tout au long du projet.

« Rapport du projet »: Le rapport détaillé de notre projet, qui présente les étapes du projet CTF, les défis rencontrés, ainsi que les solutions appliquées. Ce rapport sert de documentation complète sur le processus du projet, y compris des analyses théoriques et pratiques.

5.2. Vidéos Solutions sur GitHub

« Video-Solution »: Ce dossier regroupe les vidéos explicatives pour chaque CTF. Ces vidéos montrent les étapes de résolution des défis, offrant un guide visuel pour aider les participants à comprendre comment aborder chaque challenge et à résoudre les problèmes rencontrés.