ZAIRI Karim
DANFAKHA Abdou

Rapport du Forum Cybersécurité

Avril 2025

Sommaire

Introduction

Dans le cadre de notre formation de première année en BTS SIO (2024-2025), et plus précisément lors des Ateliers Professionnels (AP), nous avons participé à un projet déjà existant : le Forum CyberSécurité, mis en place l'année précédente.

Ce projet a pour objectif de concevoir plusieurs ateliers thématiques traitant de différents aspects de la cybersécurité. Il s'agit notamment de la protection des appareils, des réseaux et des données personnelles contre les menaces et attaques malveillantes. Le forum a une visée informative, préventive et éducative autour de ces enjeux cruciaux du numérique.

Ainsi, le projet a pour ambition de sensibiliser le public à l'importance de la sécurité en ligne, en mettant en lumière les bonnes pratiques à adopter dans notre usage quotidien d'Internet.

Plusieurs groupes d'étudiants ont été répartis sur les différents ateliers proposés. En ce qui nous concerne, nous étions en charge de l'atelier portant sur le thème des mots de passe.

ZAIRI Karim
DANFAKHA Abdou

Objectif de l’atelier : Attaque par mot de passe

Notre atelier consiste à montrer pourquoi les mots de passe solides sont essentiels. À travers une simulation, nous démontrerons aux participants qu'un mot de passe faible peut être facilement retrouvé aujourd'hui. Nous expliquerons ensuite les risques associés, tels que l’usurpation d’identité ou le vol de données.

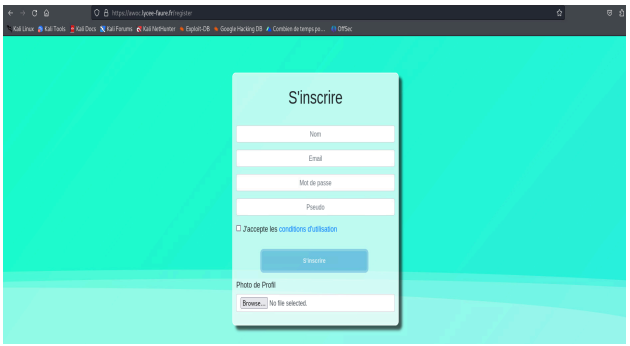
Après cette phase de sensibilisation, nous présenterons différentes méthodes de prévention pour aider les participants à mieux protéger leurs comptes. Concrètement, nous leur donnerons des conseils pratiques pour créer des mots de passe robustes ainsi que quelques astuces pour renforcer leur sécurité.

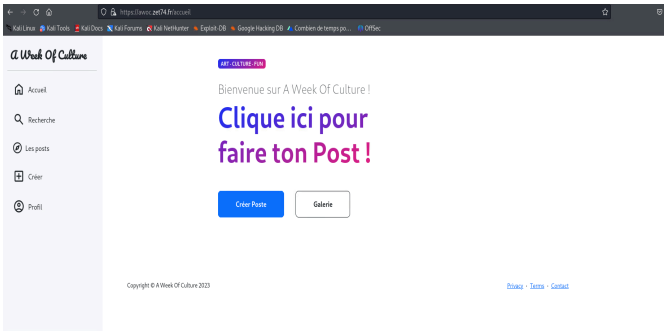
ZAIRI Karim
DANFAKHA Abdou

Scénario

Lors de l'accueil des participants dans notre atelier, nous commençons par expliquer en quoi il consiste : l’attaque par mot de passe.

Pour illustrer cela, nous proposons à un volontaire du public de se mettre dans la peau d'un utilisateur classique en s'inscrivant sur un site factice que nous avons mis en place. Lors de cette inscription, nous lui demandons de choisir un mot de passe relativement simple tel que leur couleurs préférées.





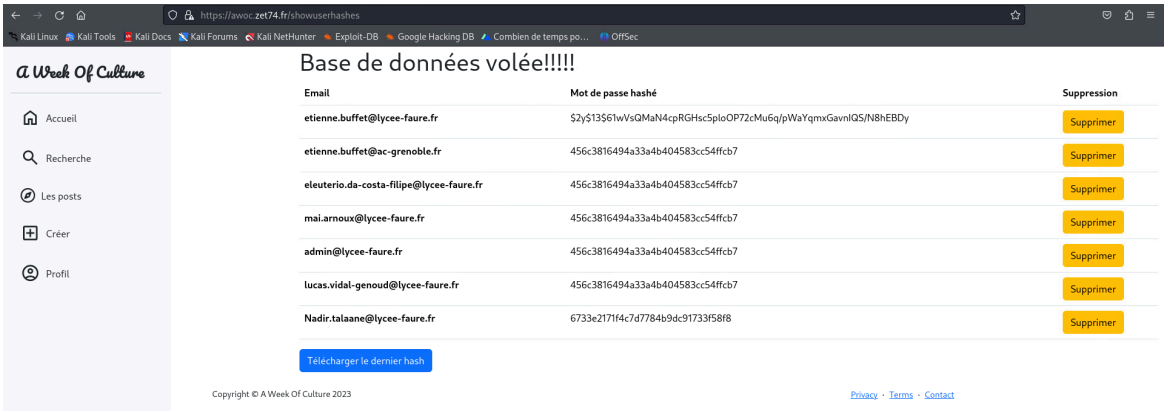
À partir de là, nous expliquons quelques notions essentielles en cyber sécurité :

- Ce qu'est une base de données ;
- Ce qu'est le hachage ;
- Le fonctionnement de l'outil John The Ripper ;
- Ce qu'est une attaque par dictionnaire ;
- La notion de dictionnaire utilisé dans les attaques ;
- Le rôle d’un algorithme de hachage.

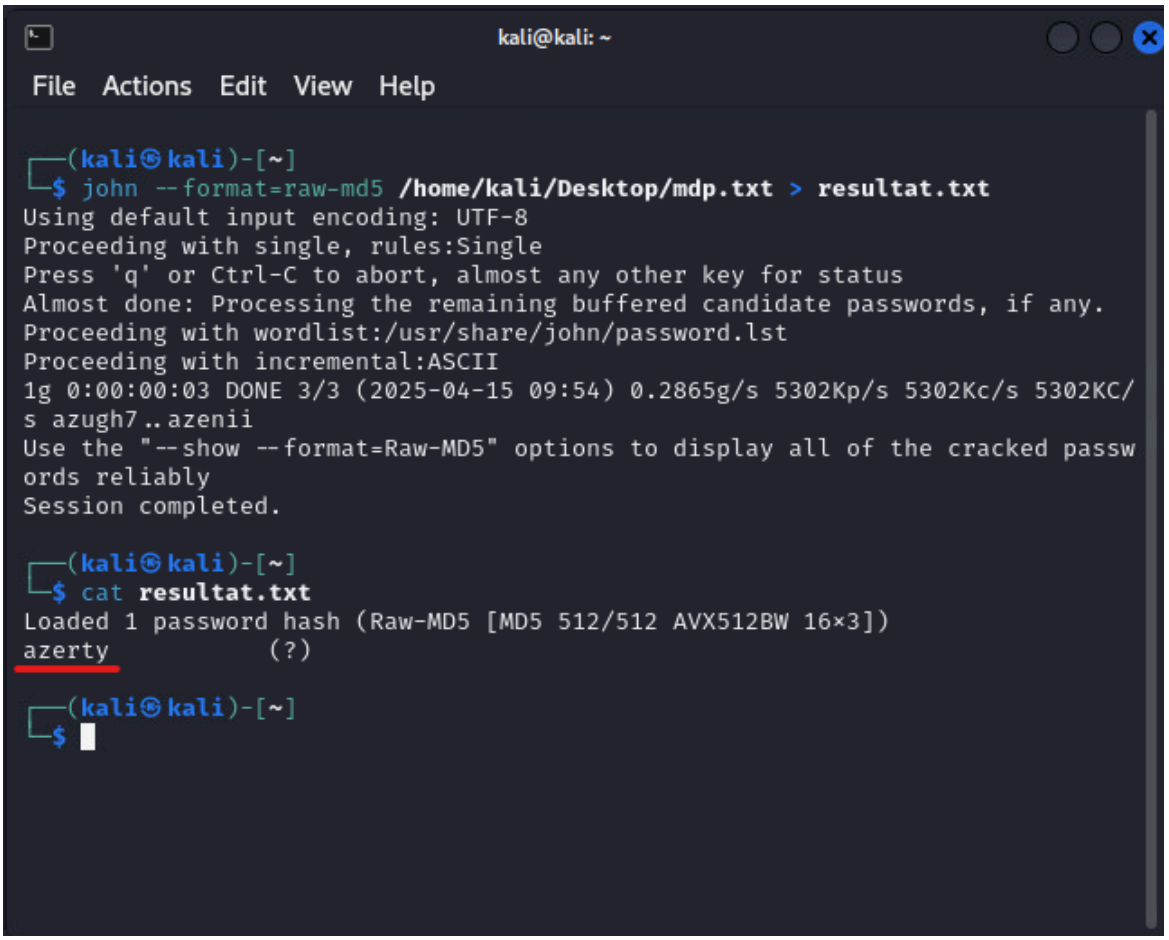
Pendant qu’un des membres de l'atelier explique ces notions aux participants, l’autre réalise en parallèle les différentes commandes nécessaires pour la démonstration.

Nous précisons et nous leur montrons que, derrière notre site, nous avons mis en place une base de données regroupant tous les

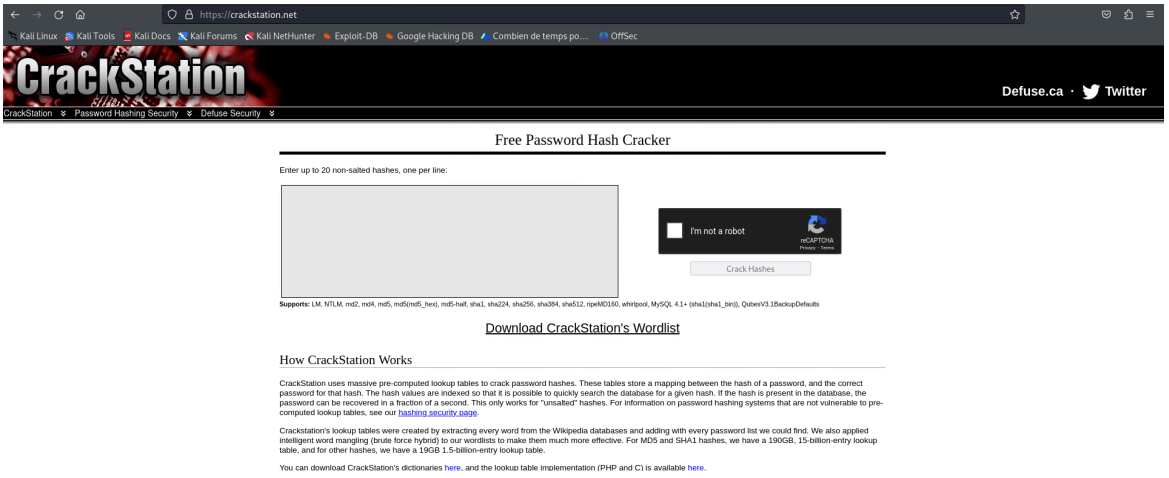
utilisateurs enregistrés, où leurs mots de passe ne sont pas enregistrés en clair, mais sous forme de hachage.



C'est à partir de ces hachages que nous récupérons les informations nécessaires pour lancer une attaque de type dictionnaire en utilisant John The Ripper, dans le but de retrouver le mot de passe du volontaire.

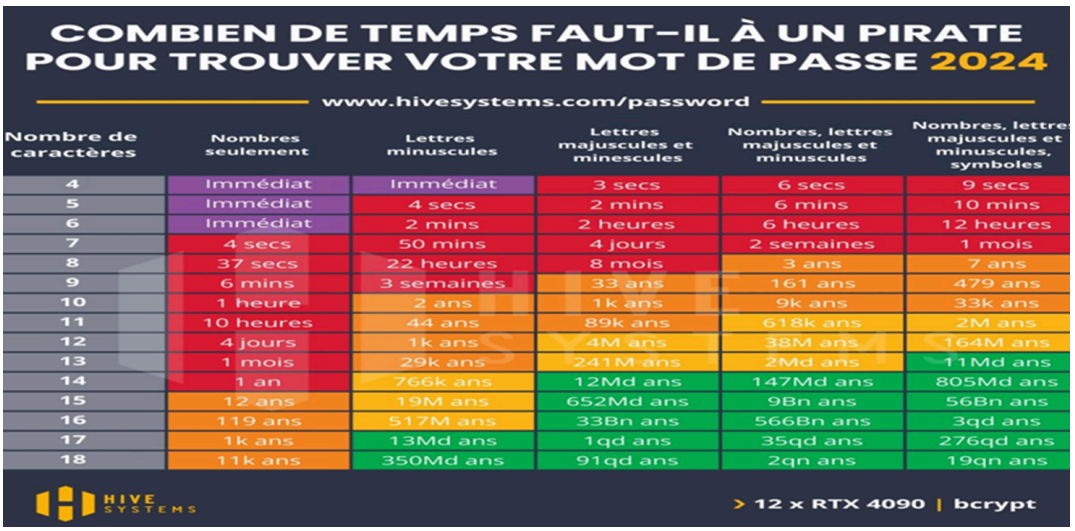


Si le mot de passe est trop complexe pour être craqué rapidement avec John The Ripper, nous utilisons alors un second outil, Crackstation, qui fonctionne de manière similaire, mais de façon plus simple et automatisée et qui a la capacité de craquer des mots de passe un peu plus compliqués, sans nécessiter de commandes.



Une fois la simulation terminée, nous sensibilisons les participants aux risques liés à l'utilisation de mots de passe faibles, comme le vol de comptes, de données sensibles ou encore l'usurpation d’identité. Nous appuyons notre discours avec des statistiques sur les principales causes de piratage et une charte illustrant combien un mot de passe faible peut être cassé rapidement, tandis qu'un mot de passe complexe résiste beaucoup plus longtemps aux tentatives de piratage.

Une étude réalisée par les experts de Kaspersky révèle que près de la moitié des mots de passe peuvent être devinés par les cybercriminels en moins d'une minute. Les conclusions du rapport, passant au crible 193 millions de mots de passe mis à disposition sur le Dark Web, piratés par des infostealers, par force brute, ou via des algorithmes intelligents, sont édifiantes.



COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

www.hivesystems.com/password

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans

HIVE SYSTEMS

> 12 x RTX 4090 | bcrypt

Le chiffre fait froid dans le dos : 1.089.342.532 mots de passe ont été volés en 2024. Oui plus d'un milliard au cours des douze derniers mois ! C'est ce que révèle le rapport Specops qui vient d'être publié. Le fournisseur de solutions de gestion de mots de passe et d'identification tire la sonnette d'alarme et invite les internautes à renforcer leurs identifiants sur le Web.

Nous expliquons également comment créer un mot de passe robuste :

- Utiliser un mot de passe d'au moins 12 caractères ;
- Présence de majuscules, minuscules, chiffres et caractères spéciaux
- Éviter les informations personnelles ;
- Ne pas réutiliser le même mot de passe sur plusieurs sites.

Enfin, nous abordons deux outils essentiels pour renforcer la sécurité : nous demandons d'abord aux participants s'ils connaissent le gestionnaire de mots de passe ainsi que l'authentification à double facteur, puis nous leur expliquons leur fonctionnement et leur utilité. L'utilisation d'un gestionnaire de mots de passe pour générer et stocker des mots de passe forts, l'authentification à double facteur,sécurité qui permet de se connecter en deux étapes

Pour clôturer l'atelier, nous proposons un QCM rapide afin de vérifier que les notions expliquées ont bien été assimilées.

ZAIRI Karim
DANFAKHA Abdou

Définitions

Base de données:

Une base de données, c'est comme un gros classeur numérique où on range plein d'informations de manière organisée pour pouvoir les retrouver facilement. Par exemple, une base de données peut contenir tous les clients d'un magasin, avec leur nom, prénom, adresse, numéro de téléphone, etc.

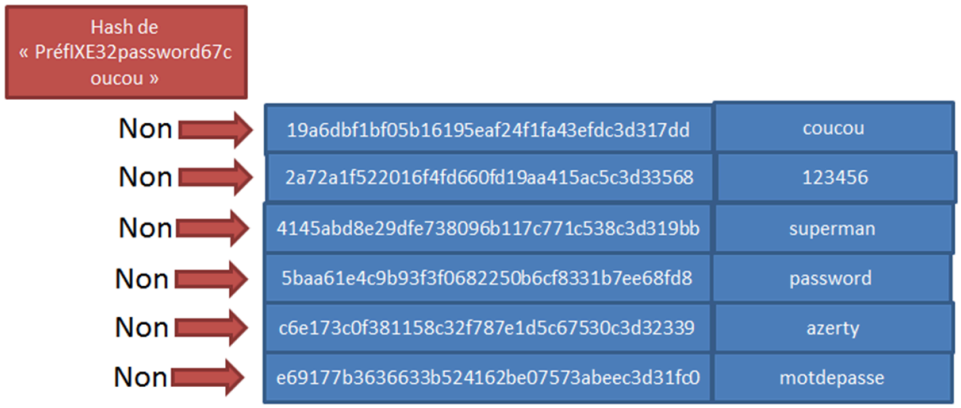
Ce système permet de **stocker, trier, rechercher, modifier ou supprimer** des infos très rapidement, même s'il y en a des milliers. Pour gérer tout ça, on utilise un logiciel spécial qu'on appelle un **SGBD** (comme MySQL ou PostgreSQL).

Les données sont souvent rangées dans des **tables**, un peu comme des feuilles Excel avec des lignes et des colonnes. Chaque ligne correspond à une fiche (comme un client), et chaque colonne contient une info spécifique (comme le prénom, l'adresse, etc.).

Hachage:

Le hachage, c'est un mécanisme qui transforme une donnée (texte, mot de passe, fichier, etc.) en une suite de caractères unique, qu'on appelle une empreinte ou une valeur de hachage.

On fait ça à l'aide d'une fonction de hachage. C'est un peu comme une machine qui prend ce que tu lui donnes et te rend un code unique, souvent en chiffres et lettres.



John the ripper:

John the Ripper est un outil qui permet de retrouver un mot de passe à partir de son empreinte cryptée, qu'on appelle un hash. Il fonctionne en testant automatiquement une grande quantité de mots de passe possibles, qu'il transforme lui aussi en hash, puis il compare ces résultats au hash à casser. Lorsqu'il trouve une correspondance, cela signifie qu'il a retrouvé le mot de passe d'origine. Il peut utiliser plusieurs méthodes pour y parvenir, comme des listes de mots courants, des combinaisons générées caractère par caractère, ou encore des variantes intelligentes de mots (avec des majuscules, des chiffres, etc.). Cet outil est principalement utilisé pour tester la robustesse des mots de passe et identifier ceux qui sont trop faciles à deviner.

Attaque par dictionnaire:

Une attaque par dictionnaire est une méthode utilisée pour retrouver un mot de passe en testant successivement chaque mot présent dans une liste prédéfinie, appelée dictionnaire. Cette liste contient généralement des mots de passe courants, des prénoms, des dates, ou des combinaisons souvent utilisées par les gens. Le fonctionnement est simple : chaque mot du dictionnaire est transformé en hash (comme le mot de passe original), puis comparé au hash à casser. Si les deux correspondent, cela signifie que le mot

de passe a été trouvé. Cette attaque est beaucoup plus rapide qu'une attaque par force brute, car elle se concentre sur les mots les plus probables au lieu de tester toutes les combinaisons possibles.

Dictionnaire:

Une attaque par dictionnaire, c'est une technique pour deviner un mot de passe en essayant une liste de mots courants. L'ordinateur teste chaque mot un par un (comme "123456", "azerty", "motdepasse", etc.) jusqu'à trouver celui qui fonctionne. C'est plus rapide que de tester toutes les combinaisons possibles, car ça commence par les mots que les gens utilisent le plus souvent.

Algorithme de hachage:

Un algorithme de hachage, c'est une méthode qui prend une information (comme un mot ou un fichier) et la transforme en une suite de lettres et de chiffres unique et de taille fixe. Peu importe la taille de ce que tu donnes au départ, le résultat sera toujours un code de la même longueur. C'est utilisé pour protéger ou vérifier des données, car on ne peut pas retrouver facilement l'information d'origine à partir du code.

Il existe différents algorithmes, certains plus rapides mais moins sécurisés (comme MD5), et d'autres plus lents mais plus sûrs (comme SHA-256). La sécurité dépend de la difficulté à retrouver l'information d'origine à partir du code, et plus l'algorithme produit un hash long, plus il est difficile à casser. En résumé, chaque algorithme a ses avantages et inconvénients en fonction de l'usage qu'on en fait.

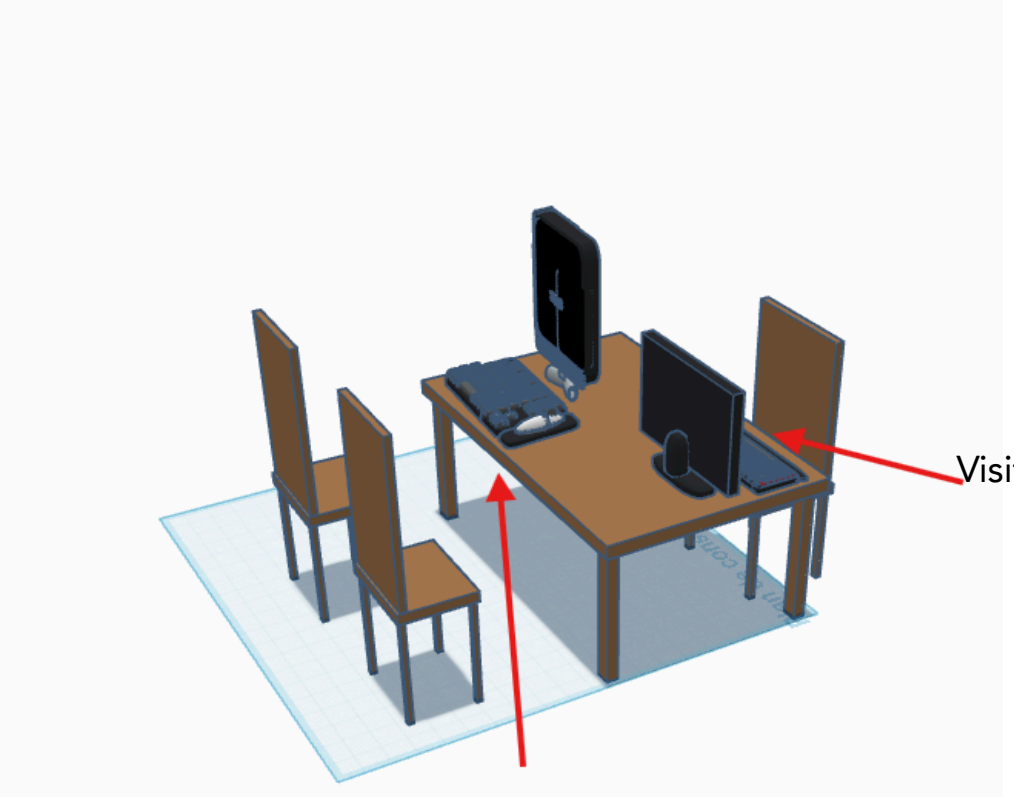
Dispositions de l'atelier

Pour la réalisation de notre atelier, nous allons utiliser ces éléments:
-2 Machines
-Windows 10 ou 11 : sur cette machine, le spectateur pourra participer à la
Première partie de notre simulation.
-Linux (Distribution Kali) dit Kali Linux : sur cette machine, nous allons pouvoir
faire la deuxième partie de notre simulation.

-Outils
-John The Ripper : un paquet* disponible sur la machine Kali Linux qui nous
permettra d'effectuer la simulation.
-Sites Web pour la simulation
Première partie
-Login : https://awoc.lycee-faure.fr/
-Création de compte : https://awoc.lycee-faure.fr/register
-Page d'accueil : https://awoc.lycee-faure.fr/accueil
Deuxième partie
Base de données : https://awoc.lycee-faure.fr/showuserhashes

Sites d'assistance
■ Crack Station : https://crackstation.net/ : ce site sert à cracker un hachage pour obtenir les données qui se cachent derrière celui-ci

Schéma



Pendant l'atelier, le visiteur s'inscrivait simplement sur le site, et une fois l'inscription terminée, il n'avait plus rien à faire. Ensuite, grâce au partage d'écran, il pouvait suivre ce que faisait l'autre membre du groupe, qui tapait les commandes sur l'ordinateur. Un des deux présentateurs était debout et expliquait en temps réel les actions effectuées, les commandes tapées, ainsi que les attaques et les concepts de sécurité liés, tout en permettant au visiteur de suivre visuellement ce qui se passait.

Point d’amélioration

-Rendre le site factice plus réel afin d’immerger les visiteurs, de rendre les démonstrations plus percutantes, de renforcer la prise de conscience des risques, et de valoriser le travail en montrant un projet plus professionnel et crédible.

-Améliorer l’organisation de l’espace de travail : mieux disposer le matériel et structurer l’accueil permettrait d’avoir un atelier plus fluide, plus clair pour les visiteurs et plus professionnel dans sa présentation.