Projet CTF - Cahier des charges

Projet

Comme projet, nous avons décidé de faire une plateforme CTF (Capture the Flag). Il s'agit d'événements de cyber-sécurité. Ils peuvent avoir lieu en ligne ou en présentiel. Afin de participer à un CTF, une plateforme permet à des utilisateurs de se connecter et de fonder des équipes. Les équipes peuvent participer à des CTF de plusieurs types : jeopardy et attaque-défense.
Pour les CTF de types jeopardy : les utilisateurs doivent résoudre un maximum de challenges de sécurité informatiques. Ces challenges peuvent être en plusieurs étapes (il faut trouver un code appelé flag et le soumettre à un validateur), lorsqu'une équipe trouve un flag, l'équipe remporte un nombre de points qui s'ajoute à ceux déjà obtenus durant le challenge.
Pour les CTF de types attaque-défense : chaque équipe se voit attribuer une machine avec un flag dedans qu'elle doit protéger, son but est de récupérer celui des autres équipes.

Besoins en données

Afin de réaliser correctement ce projet, nous aurons besoin des données mentionnées ci-dessous. La liste des données est divisée selon les différents acteurs et fonctionnalités que nous souhaitons implémenter.

Utilisateurs

Chaque utilisateur possède un compte qui est composé de son pseudonyme (unique), son adresse e-mail (unique), un mot de passe, une description (optionnelle), l'URL de son site internet (optionnel). Si l'utilisateur rejoint une équipe, celle-ci est aussi mentionnée sur son profil.
Les utilisateurs peuvent avoir un rôle : user ou admin.

Equipes

Une équipe possède un nom (unique), un mot de passe pour accéder à celle-ci, le pseudonyme de son créateur, la liste de ses membres, un type (pro, student, etc…).

Événements CTF

Un CTF a un nom et il peut être soit physique (hors-ligne), soit en ligne, s'il est physique, des salles y sont attribuées. Il peut aussi être de deux types, soit attaque-défense, soit jeopardy. L'événement est limité dans le temps.

Challenges type attaque-défense

Un challenge de type attaque-défense possède, une équipe, un flag et un serveur.

Challenges et étapes type jeopardy

Un challenge possède un nom (unique), une description, un type (réseau, programmation, forensic, etc…), un auteur/créateur, une date de création, une date de fin et la liste des étapes qui le compose.

Un challenge est composé de plusieurs étapes, chaque étape possède un nom (unique au sein du challenge), une description, un nombre de points, un barème de difficulté (1-5) et un flag (= un mot de passe) qui permet de valider le challenge.

Salles

Une salle a un étage et un numéro associé.

Serveurs

Certains challenges doivent être hébergés sur un serveur. Ces serveurs sont identifiés par leur adresse locale, leur numéro d'identification, leur mainteneur ainsi que la salle dans laquelle ils se trouvent.

Writeups

Un writeup a un titre et un contenu. Il est lié à un challenge de type jeopardy en particulier et à un utilisateur. Le writeup peut être écrit AVANT la fin de l'événement mais PEUT être visible uniquement APRÈS la fin du CTF.

Fonctionnalité

Utilisateurs

Les utilisateurs peuvent créer des comptes et se connecter s'ils en possèdent déjà un. Chaque compte utilisateur est unique, il ne doit donc pas y avoir deux fois soit le même pseudonyme, soit la même adresse e-mail.

Un utilisateur peut créer une équipe et gérer celle-ci (détails dans le sous-chapitre sur les équipes). Les autres utilisateurs peuvent rejoindre l'équipe en cherchant le nom de celle-ci dans un outil de recherche et en rentrant le mot de passe qui lui est associé.

Administrateur

- Un administrateur qui est un utilisateur avec un rôle d'administrateur peut créer des challenges de type jeopardy pour les autres utilisateurs. Il dispose d'une interface où il peut rentrer les détails de ceux-ci (détails dans le sous-chapitre sur les challenges)
- Un administrateur peut créer des challenges de types attaques défense.
- Un administrateur peut créer des évènements CTF.

Équipes

Chaque utilisateur peut créer son équipe en rentrant les informations citées précédemment. Les autres utilisateurs peuvent rejoindre celle-ci, s'ils possèdent le mot de passe associé. La limite maximum de participants dans une équipe est de 4 membres (créateur compris).

Les créateurs peuvent gérer l'équipe, c'est-à-dire gérer les membres présents dans celle-ci pour les virer si besoin. Ils peuvent aussi changer le mot de passe qui avait été fixé lors de la création. Le créateur est celui qui inscrit l'équipe au différents challenges.

Chaque équipe possède une page où on y voit afficher ses informations, les membres et les points totaux qu'elle a pu acquérir en réalisant divers challenges.

Challenges et étapes

Un administrateur commence par créer le challenge dans un premier temps en fournissant les informations requises, puis dans un second temps il ajoutera les étapes qui le composent.

La fonctionnalité principale est la validation des challenges. Lorsqu'une équipe est inscrite, elle possède l'opportunité de valider les diverses étapes qui composent le challenge en rentrant le flag (un flag par étape pour les types CTF jeopardy, un flag par machine pour de l'attaque-défense). On ajoute ensuite les points de l'étape aux points courants que possède l'équipe sur ce challenge. Une équipe ne pouvant pas valider plusieurs fois le même flag.

Il est important de préciser que le temps n'est pas infini, chaque challenge à une date à laquelle il se termine. Après cette date, il n'est plus possible de soumettre de réponse pour les étapes et le challenge est verrouillé pour toujours.

Writeups

À la fin d'un événement CTF de type jeopardy la liste des writeups s'affiche sur la page d'un challenge.