Escape game de l'informaticien

Les Capture The Flag (CTF) sont des challenges de sécurité informatique. Souvent proposés en temps limités lors de conventions ou événements particuliers, ils prennent souvent forme de machine virtuelle, de serveur accessible en ssh ou simplement d'un page web. Le but est alors d'exploiter des vulnérabilités plus ou moins évidente du système, afin d'obtenir des *drapeaux*. Ceux-ci prennent souvent la forme d'un fichier auquel il n'est à priori pas possible d'accéder (fichier protégé par un mot de passe, appartenant à un autre utilisateur, généré à la volée par une application ...).

La plupart des challenges CTFs proposent une difficulté progressive, avec des failles à trouver de plus en plus fines pour avancer dans le système. La progression peut prendre la forme d'accès à des comptes utilisateurs successifs, se terminant généralement par l'accès au compte root.

La première partie de ce projet consiste à "jouer" à certains de ces challenges, ou plutôt se heurter à eux dans un premier temps.. Selon votre motivation, plusieurs challenges de difficulté progressive sont envisageables.

Dans un second temps, vous devrez créer vous-même un CTF, contenant les défis de votre choix (entre 1 et 6 est une fourchette raisonnable). Cela demandera notamment de :

- Concevoir les failles qu'il faudra exploiter
- S'assurer qu'elles ne peuvent pas être contournées autrement
- (optionnel) apprendre à empaqueter tout ça dans une joli iso *live-CD*

Notez que but n'est pas de produire ici un CTF impossible à résoudre, mais bien de proposer un "jeu", si possible de difficulté croissante.

Si plusieurs groupes choisissent ce sujet, un échange de CTF avec ~~combats de chiens~~ challenge cordial entre groupes sera bien sûr envisageable.

Références.

- Wikipédia CTF : `https://en.wikipedia.org/wiki/Capture_the_flag#Computer_security`
- Ressources autour du CTF : `https://github.com/ctfs/resources/`
- Plus de ressources : `https://resources.infosecinstitute.com/tools-of-trade-and-resources-to`
- Challenges de tous niveaux en ssh : `https://pwnable.kr/`