Hacking et Pentesting

Mars 2021 | **Serie 3**

Stéphane Küng

1 Administratif

Ce travail **individuel** doit être rendu avant la date indiquée sur le ScoreBoard au format **PDF** sur CyberLearn.

Dans vos rapports d'exercices, faites attention à bien inclure:

- Captures d'écran de réussite
- Payload utilisés
- Tout **code source** utilisé ou créé (ou en annexe)
- Nom des outils utilisés
- Configuration

2 Exercices LD_PRELOAD

2.1 Voyance 1

Le projet `Voyance` à pour but de repérer les étudiants disposants d'un don de clairvoyance et capables prédire l'avenir.

Nous utilisons pour ca le binaire `./voyance1`. Il génère un mot de passe aléatoire sur la base de plusieurs souces à chaque lancement. Si l'étudiant possède de tels dons, il sera capable de prédire le mot de passe avant l'execution de ce binaire.

Veuillez rendre, avec le rapport, le **code source** de vos fonctions LD_PRELOAD (en annexe dans un `.zip/.7z` ou dans le PDF du rapport).

2.2 Voyance 2

Suite à des tentatives de triche de la part d'étudiants ne disposant d'aucun don avec le `LD_PRELOAD`, la ligne suivante a été ajoutée au démarrage, ça devrait les décourager.

```
1 if (rand()==rand() && rand()==rand()) {
2     printf("Error, something wrong with the random number generator\n");
3     exit(2);
4 }
```

2.3 Voyance 3 (Difficile)

Suite à de nouvelles tentatives de triche, le binaire a été renforcé avec de multiples vérifications.

3 Exercices de modification mémoire

3.1 Age Of Empire 1

Le jeu Age of Empire trop est difficile voir impossible. Utiliser un éditeur de mémoire pour obtenir un chateau. Documenter comment vous avez fait, les outils utilisés et ce que vous avez modifié. Mettez votre

code chateau dans le rapport `PDF`

3.2 Age Of Empire 2 (Difficile)

Le jeu Age of Empire trop est difficile voir impossible. Coder, avec les fonctions vues en cours (ptrace) un programme (aussi appellé `trainer`) vous permettant d'automatiser la modification des mémoires du jeu. Documenter votre analyse et envoyer votre code source joint au rapport `PDF`