Hacking et Pentesting

Mars 2021 | **Serie 4**

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 Modification de code

2.1 Age Of Empire 3

Modifier le jeu Age of Empire (Série 3) de sorte qu'il distribue plus de ressource lorsque l'utilisateur en demande. Le jeu doit continuer à fonctionner.

2.2 CrackMe4 .Net 1

Décompiler le CrackMe4.exe pour le comprendre et modifiez le si besoin. Donner votre solution, celle-ci doit fonctionner sur la version **non modifiée** du binaire.

2.3 CrackMe4 .Net 2

Modifier le CrackMe4.exe de sorte que votre prénom soit la solution du binaire. Documenter la modification apportée.

3 Exercices Side Channel Attack

3.1 CrackMe 5 - Time Attack

Le CrackMe 5 est vulnerable à une timming attack. Le but de cet exercice est de coder un script ou application qui teste toutes les combinaisons possibles. Le CrackMe vérifie chaque caractère dans l'ordre, si un cactatère est bon, il passe au suivant. Testez toutes les possibilités sur le premier caractère puis une fois trouvé passez au suivant. Quelle que soit la tentative, le mot de passe doit faire X caractères

4 Exercice Injection

4.1 DLL Injection

Injecter dans la DLL du CrackMe6 un `Meterpreter`, de sorte qu'il fonctionne et soit chargé lors du lancement du binaire. Tester le avec la console m`msf`