**TP Bonus: Crack my owl**

Dans ce TP de reverse engineering, vous allez analyser et tenter de craquer plusieurs binaires "crackme" afin de découvrir les mots de passe requis. L’objectif principal est de documenter les étapes suivies, les outils utilisés, les difficultés rencontrées, et les méthodes employées pour trouver les mots de passe. Le rendu devra être méthodique, avec une attention particulière portée à la documentation. La qualité des explications méthodologiques est essentielle pour obtenir des points.

### Objectifs :

* **Identifier le mot de passe :** Chaque binaire doit être exécuté avec un mot de passe en argument. Le mot de passe correct sera validé si le programme affiche "OK\n" sur la sortie standard et retourne 0.
* **Méthodologie :** Détailler les étapes de reverse engineering employées pour trouver chaque mot de passe. Si un rapport contient uniquement les mots de passe sans explications méthodologiques, il sera noté zéro.

#### Crackme Simples (1.25 pts + 1.25 pts par mot de passe trouvé) :

Les exercices simples sont les suivants : 05, 06, 07, 08, et 09.  
Pour chacun de ces crackmes :

* **Documentation :** (1.25 pts) Documentez précisément les étapes de reverse engineering, les outils utilisés, et les commandes exécutées. Incluez des notes sur les fonctions identifiées, les structures de contrôle (boucles, conditions), ainsi que toute information pertinente.
* **Mot de passe :** (1.25 pts supplémentaires) Trouvez le mot de passe requis par le programme. Le mot de passe doit être correctement identifié pour obtenir ces points.

#### Crackme Avancé : owl (3.75 pts + 3.75 pts si le mot de passe est trouvé)

L'exercice "owl" est plus complexe et nécessite une analyse approfondie :

* **Documentation :** (3.75 pts) Identique, prenez également des notes sur les difficultés rencontrées, les hypothèses testées, et les méthodes d'investigation.
* **Mot de passe :** (3.75 pts supplémentaires) Trouvez le mot de passe ou décrivez en détail les progrès réalisés et les obstacles rencontrés. Les points ne seront attribués pour cette partie que si le mot de passe est trouvé.

### Instructions Générales :

1. **Analyse Dynamique et Statique :**
   1. Utilisez des outils tels que gdb-gef, Ghidra, ou tout autre désassembleur/débogueur pour analyser les binaires.
   2. Essayez de comprendre le processus de vérification du mot de passe. Cela inclut l’analyse des fonctions, boucles, et instructions clés.
2. **Documentation des Étapes :**
   1. Notez chaque outil et commande utilisé, les adresses de mémoire intéressantes, les résultats des étapes d’analyse, et les hypothèses testées.
   2. Suivez une démarche progressive et structurée, en procédant par étapes pour ne pas vous égarer.
3. **Prise de Notes Générales :**
   1. Documentez les difficultés rencontrées, les incompréhensions, et les doutes tout au long de votre processus. Ces notes doivent refléter les obstacles majeurs et les questionnements.

### Format de Rendu :

Le rendu final devra être un fichier DOC ou PDF comprenant les éléments suivants :

* **Documentation Détailée :** Les étapes méthodologiques suivies, les outils et les commandes utilisés, ainsi que les notes explicatives sur chaque exercice.
* **Page de Résumé :** La première page doit contenir, de manière très visible, un résumé des résultats sous la forme suivante (Si cette condition n'est pas respectée, un malus sera appliqué à la note finale):
* ./05 <MDP>
* ./06 <MDP>
* ./07 <MDP>
* ./08 FAIL
* ./09 <MDP>
* ./10 FAIL

### Notation (Total sur 20) :

* **Exercices Simples :** 5 exercices, chacun noté sur 2.5 (1.25 pts pour la méthodologie et 1.25 pts pour le mot de passe, uniquement si le mot de passe est trouvé).
* **Exercice owl :** 7.5 pts (3.75 pour la documentation de qualité et 3.75 supplémentaires uniquement si le mot de passe est trouvé).

**Conseils :**

* **Patience et Méthode :** Respectez une démarche progressive pour maximiser vos chances de réussite.
* **Utilisation des Outils :** Profitez des fonctionnalités des outils comme Ghidra (clic droit sur les fonctions, analyse des graphes) pour vous faciliter la tâche.

En suivant cette approche, vous devriez pouvoir progresser efficacement dans le crack des binaires proposés. Soyez prêt à partager et à discuter vos méthodes lors des prochaines séances.