Introduction à l'ingénierie inverse

Cet atelier consiste a « cracker » un programme dont un mot de passe est nécessaire pour y accéder. A l'aide d'un logiciel nommé Ghidra, vous allez apprendre:

- Les fonctionnalités de base de Ghidra
- A vous familiariser un peu plus avec le concept de la mémoire et d'adresses
- Lire un peu d'assembleur, et même en écrire
- Faire la passerelle entre le code source et l'assembleur
- Quelques techniques pour vous permettre de « cracker » un programme

Le but de cet atelier étant de vous familiariser avec un exemple simple, aucun code source sera présent dans l'archive. Il faudra donc faire preuve de créativité, et de logique. (Et un peu de googling, évidemment).

Dans le dossier src se trouve le programme. Vous aurez trois « exercices » à réussir, bien que vous n'êtes pas obligé de tous les faire.
J'aimerais introduire le concept d'évaluation pour cet atelier. Vous n'aurez pas de point, mais je peux m'arranger pour un cookie.Si vous décidez de jouer le jeu de l'évaluation, voici comment se passera la remise:

- Créez un dossier « atelier_eval ». Dans ce dossier, vous allez créer vos dossiers ex00, ex01..(voir plus bas pour les voir) et mettre dans chaque dossier le/les fichiers correspondants.
- L'évaluation se fera sur le poste de l'évalué
- L'évalué, pour chaque exercice fait, devra expliquer son processus pour arriver a son résultat. L'évaluateur devrait recevoir des explications claires.
- Si un programme est remis, l'évalué doit lancer son programme et montrer qu'il a bien été modifié, puis ouvrir le programme avec Ghidra et expliquer a l'évaluateur son processus et méthodes pour arriver au résultats.
- 1 évaluation nécessaire (ou plus si vous voulez). Si vous voulez une moulinette, j'assumerais(llaplant)le role.

Ex00:

Vous devez trouver le bon mot de passe, a l'aide de Ghidra, et mettre votre réponse dans le fichier ci-dessous.

- Fichier a remettre: password.txt

Ex01:

Vous devez changer le mot de passe pour votre login, suivi de 42. (Ex: llaplant42).

- Fichier a remettre: AnswerTo42_patched1

Ex02:

Vous devez patcher le programme pour qu'il vous laisse entrer, peu importe l'input que vous lui donnez.

- Fichier a remettre: AnswerTo42_cracked

Partie 2

Cette partie est une partie « bonus ». Dans le dossier src, il y a un deuxième programme nommé « FallingWhale ». Comparé au premier programme, celui-ci est d'une difficulté assez modérée. Pour cette partie, il faudra remettre en une seule fois:

- Un fichier contenant une documentation sur le fonctionnement du programme
- Un keygen écrit en C (doit être écrit a la norme, outre la règle des 25 lignes et 5 fonctions) qui devra permettre de générer une clé fonctionnelle pour le vrai programme

Note: Il se pourrait très bien que Ghidra exporte votre programme avec l'extension « .bin ». Pas de panique, vous pouvez renommer l'exécutable pour enlever l'extension sans problème, le programme (si vous avez bien fait le travail) se lancera dans le terminal.

Happy cracking !