Enigme système : niveau 4

12 janvier 2017

1 Le background

Le background de l'énigme 3 s'applique à bon nombre de cas, par exemple à tous les jeux où il faut taper une clé (style chaîne de caractères) pour débloquer l'accès au niveau suivant. Il y a 30 ans, parmi les gamers, il y avait des hackers qui avaient les compétences suffisantes pour explorer l'exécutable du jeu et trouver comment le jeu vérifiait les clés saisies par le joueur.

Ces hackers se faisaient des outils maison pour faire cette recherche, ou bien utilisaient un débogueur grâce auquel ils identifiaient les morceaux de code exécutable correspondant à la vérification de la clé saisie par le joueur. Mais bien souvent, les développeurs de jeux ne cherchaient pas de moyens compliqués pour masquer ces clés et elles étaient stockées dans l'exécutable telles quelles. Il fallait simplement trouver où.

2 L'énigme

Connectez-vous sur le serveur, à partir d'une machine de l'IUT : `ssh level4@domjudge`

Vous tapez le mot de passe trouvé à l'énigme 3. Vous êtes alors logué avec comme répertoire courant la racine `/` du système de fichiers. Déplacez-vous dans votre home directory : `cd /home/hacker`.

L'executable `hackworld` est le pseudo-jeu qui vous demande de saisir une clé pour le niveau suivant. Si vous tapez la bonne clé, un message vous indiquera le mot de passe du niveau 5.

Indice 1 : dans un exécutable, il y a des **sections** contenant différents types de données (code exécutable, variables globales, ...). Par exemple, toutes les **chaînes de caractères constantes** (par exemple, `char* msg="salut"`, `printf("bonjour");` ...) sont regroupées dans une même section.

Indice 2 : `objdump` est ton ami.

3 les ressources

Pour vous aider dans la réalisation du programme, vous trouverez sur
`http://cours-info.iut-bm.univ-fcomte.fr`

un article dans la section `hackaton` → `édition 2017`, portant le même titre que l'exercice. Il contient un lien permettant de télécharger un canevas de code permettant de comptabiliser la solution.