HACKING DE FICHIERS ET DE PROGRAMMES

Nous allons apprendre à éditer des fichiers binaires de données d'applications. Pour ce faire nous allons utiliser une application nommée HxD qui permet d'éditer les fichiers et de voir leur contenu en hexadécimale. Cet éditeur permet aussi de comparer deux fichiers afin de comprendre ce qui diffère si on change quelque chose à l'intérieur d'un fichier.

Le programme à « hacker » aujourd'hui s'appel « Test.exe » et c'est une application qui enregistre une somme d'argent qui vous appartient. Cette somme d'argent n'est modifiée que si vous appuyez sur le bouton « Récolter de l'argent ». Lorsque le programme se ferme il enregistre automatiquement les données, et lorsqu'il se lance il les charge.

1) Téléchargez et décompressez HxD
2) Lancer le programme « Test.exe » et comprenez son fonctionnement
3) Récolter un peu d'argent puis quitter le programme, un fichier « Test.data » devrait être créé avec les données à l'intérieur
4) Renommer ce fichier en « Test2.data » et relancez le programme. Récolter un peu d'argent pour avoir un montant différent puis quitter le programme.
5) Vous devriez maintenant avoir 2 fichiers .data avec 2 valeurs d'argent différentes
6) A l'aide de HxD, ouvrez les deux fichiers et comparez-les avec la fonctionnalité prévue à cet effet (Analyse -> Comparaison de fichiers)
7) Trouvez l'adresse correspondante au montant puis changer la somme par le montant que vous désirez. Vous pouvez calculer le montant que vous voulez avec la calculatrice windows en mode programmeur qui permet de faire des conversions décimale -> hexadécimale (par exemple en changeant la valeur 001A soit une somme de 26 en décimal en FFFF, on obtient une somme de 65535)

Vous savez maintenant comment éditer des fichiers de données avec un éditeur hexadécimal. Vous pouvez changer n'importe quel fichier, pas uniquement les fichiers de données, essayer par exemple de changer le nom d'un programme que vous avez, il suffit d'ouvrir le .exe et de rechercher le nom à l'intérieur. Des fois les noms peuvent être séparés par des points, il vous faut alors faire un rechercher avec l'option « chaîne Unicode ». Attention toutefois à ne pas changer la taille du fichier, un changement de taille provoque souvent la destruction de celui-ci.