Cours de Cracking

(2ième Partie)

Dans cette seconde partie de notre tutorial, nous allons aborder différents raisonnements pour cracker, toujours avec StartClean ... (le pauvre :( ). Dans cette partie du cours, je m'adresse particulierement aux Newbies qui ont deja essayé de cracker un truc mais qui ont pas réussi, sans comprendre pourquoi...

1/ Les logiciels utiles pour ce cours

-> Le programme à craquer : **Start Clean v1.2**
-> Un désassembleur : **W32dasm 8.93**
-> Un éditeur hexa décimal : **Winhex 10.2**

2/ Contenu d'un programme

Dans un programme il y a des menus, un titre en haut de la fenêtre, une barre d'état, des boîtes de dialogues....

Tous ces éléments contiennent du texte (menu "Fichier", "Erreur 806...") Eh ben, W32Dasm permet de retrouver ce texte a l'intérieur de l'exécutable ! C'est ce que nous avons déja fait dans la première partie du cours (souvenez vous de la recherche sur le mot "name"), sauf que maintenant, je vais expliquer un raisonnement que beaucoup de newbies ont mais qui s'avère erroné... Lorsque l'on rentre un code au pif asn start clean, on tombe sur la boîte de dialog "Incorrect Code"...

Reflechissons donc deux secondes : ce message ne s'affiche qu'a condition que le code soit faux...

Donc, si on arrive a retrouver ce message, on pourrait faire en sorte qu'il ne s'affiche plus (en "noppant" un saut conditionnel par exemple...) Essayons ce raisonnement dans W32Dasm...:

-> Lancer W32Dasm.
-> Désassembler le fichier StartClean. (cf cours de crack 1)
-> Faites Refs => String Data References.... Là, vous devriez avoir une petite fenetre comme celle ci :

Bon, balladez vous dedans jusqu'a ce que vous trouviez la phrase "Incorrect Code"...

-> Double cliquez sur cette phrase : vous êtes amené à l'endroit précis où on y fait reference ! Cependant, de la même maniere qu'il y avait plusieurs fois le mot name dans le 1er cours, verifiez que "Incorrect Code" n'est pas repeté plusieurs fois dans le programme...(double cliquez plusieurs fois dessus). Par chance, il n'y a qu'une seule occurence a cette phrase !

NB : s'il y avait eu plusieurs occurences, il aurait fallu s'occuper de chacune de ces occurences, ou alors determiner celles qui nous interressent (cf 1ere partie du cours). Bien, maintenant observons l'endroit ou on a atterri :

La ligne "Referenced by..." indique l'adresse qui nous a amené ici, c'est a dire l'adresse 004027A3 depuis laquelle le programme a sauté...Il y a un "C" entre parenthese juste derriere l'addresse. Ce "C" signifie tout simplement "Conditional". Ca veut dire que c'est un saut conditionnel qui nous a envoyé a cette partie du code.

Reflechissons un minimum : si on veut ne pas venir ici, il suffit de nopper ce vilain saut ! On va donc aller a l'adresse indiquée par le "Referenced by....", a savoir 004027A3 ...Faites :

-> Faites : Goto => Goto Code Location... (ou shift F12) et rentrer l'adresse en question : 004027A3.

Oh !! Le beau je 004027C1 !! Bon, ben vous savez ce qu'on va faire : On va nopper le saut :).

-> Dans l'éditeur hexadecimal winhex, vous aller cherchez 741C. Cependant, il va falloir mettre plus d'instructions que "741C" parcequ'il peut y avoir plusieurs fois "741C" dans le code Hexadecimal du programme :). Donc, on va cherchez "741C" en rajoutant un peu devant et un peu derriere : 83C40485C0741CC7054C7240

NB : si vous comprenez pas d'ou sorte les chiffres avant et apres, faites le rapprochemment avec le listing de la photo du dessus. Une fois la recherche effectué, vous remplacez le 741C par 9090... Maintenant, lancer le prog et enregistrer vous n'importe comment : ca marche !!! Super !!!

Etes vous sur que ca marche vraiment ? Bien sur, le programme ne vous dit plus "Incorrect Code", mais êtes vous pour autant enregistré ? Un seul moyen de le savoir : fermer le prog' et relancer le... Sniff!...ben non, ca a pas marcher :(...enfin, pas tout a fait...

Explications : en fait, tout ce qu'on a fait, c'est detourner le message sensé nous indiquez que le code est incorecte...Ce message s'affiche lorsque le programme sait deja qu'on a entré un faux code.

Reprenons les choses pas-a-pas :
-> On vous demande de rentrer un nom et un code...

-> Lorsque vous cliquez sur "OK", le programme verifie le code :
  -> s'il est bon, c'est cool et vous etes enregistrer,
  -> si il est pas bon, on vous previens par un petit message que le code est mauvais...

Donc,s'il y a le message "Incorrect Code", ca veut dire que le programme a deja determiné que le code était faux...Inutile donc d'essayer de changer le message qu'on nous affiche, c'est bien avant qu'il faut agir :) Compris ??

Si j'ai pris le temps d'expliquer cette erreur, c'est parceque beaucoup de Newbies tombent dans le piège lors de leur premiers cracks. J'espère donc que ce cours aura eclairé certains et prévenus d'autres sur les résultats d'un tel raisonnement ;)