Cours de Cracking

(12ième Partie)

Mon objectif : craquer mIRC 5.5

1/ Les logiciels utiles pour ce cours

-> Le programme à craquer : **mIRC**
-> Un désassembleur : **W32dasm 8.93**
-> Un éditeur hexadécimal : **Winhex 10.2**

2/ Présentation

Tout d'abord on peut se demander pourquoi cracker mIRC alors qu'il ne possède à proprement dit aucune
protection à part un nag screen de temps en temps.

En fait, cela constitue tout de même une bonne initiation au crack, et cela va permettre au débutants de suivre sans trop de difficultés (enfin je l'espère... :-) et leur permettrent d'acquérir quelques bases.
Ou bien encore la satisfaction de voir son nom dans la fenêtre ou l'on voit habituellement 'unlicenced'.

3/ Désassemblage et craquage

-> Allez dans mIRC et dans le menu faites 'Help' puis 'Register'.
-> Entrez votre nom et un serial bidon puis appuyez sur 'ok'.
-> Et le message : "Sorry, your registration name and numer don't match! Please..." apparaît. Notez le, il va nous servir pour la suite.
-> Puis faites une copie de mIRC32.exe en la renommant par exemple 1.exe
-> Faites en une seconde copie et renommez la en 2.exe
-> Ensuite desassemblez 1.exe avec W32dasm
-> Allez ensuite dans String Data References, et dans la liste des messages cherchez le messages d'erreurs que nous avons noté précédemment. C'est bon vous l'avez ? Ok au boulot

-> Cliquez deux fois dessus, voilà W32dasm nous emmène dans le programme ...

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
:00435D09(C) //(nous allons y faire référence un peu plus bas...)
:00435DAA 6A00            push 00000000


* Reference To: USER32.MessageBeep, Ord:0000h
:00435DAC E80B1C0900      Call 004C79BC
:00435DB1 68E9AD4C00      push 004CADE9
:00435DB6 6A00            push 00000000
:00435DB8 6A0C            push 0000000C


* Possible Ref to Menu: MenuID_0017, Item: "Search..."
* Possible Reference to Dialog: DialogID_0033, CONTROL_ID:0083,
:00435DBA 6883000000      push 00000083
:00435DBF 8B5508          mov edx, dword ptr [ebp+08]
:00435DC2 52              push edx


* Reference To: USER32.SendDlgItemMessageA, Ord:0000h
:00435DC3 E8481C0900      Call 004C7A10
:00435DC8 68EBAD4C00      push 004CADEB
:00435DCD 6A00            push 00000000
:00435DCF 6A0C            push 0000000C


* Possible Ref to Menu: MenuID_0017, Item: "Contents"
* Possible Reference to Dialog: DialogID_0033, CONTROL_ID:0082, "
:00435DD1 6882000000      push 00000082
:00435DD6 8B4D08          mov ecx, dword ptr [ebp+08]
:00435DD9 51              push ecx....


* Reference To: USER32.SendDlgItemMessageA, Ord:0000h
:00435DDA E8311C0900      Call 004C7A10
:00435DDF 6A10            push 00000010
:00435DE1 6A00            push 00000000.


* Possible Reference to String Resource ID=01912: "mIRC
Registration!"
:00435DE3 6878070000      push 00000778
:00435DE8 E81348FDFF      call 0040A600
:00435DED 50              push eax
:00435DEE 6A00            push 00000000


* Possible Reference to String Resource ID=01913: "Sorry, your registration name and
number don't match!..Pleas"
//(Le programme nous amène ici si le code est mauvais.)
:00435DF0 6879070000      push 00000779
```

```
:00435DF5 E80648FDFF      call 0040A600
:00435DFA 50              push eax
:00435DFB 8B4508          mov eax, dword ptr [ebp+08]
:00435DFE 50              push eax

* Reference To: USER32.MessageBoxA, Ord:0000h
//Il s'agit donc de savoir quand le programme décide de nous envoyer ici...
//on remonte donc pour chercher un saut conditionnel (Je ou Jne, Ja....).
//Au bout d'un moment on arrive ici : (c'est ce qui avait au tout debut...)

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
:00435D09(C)
:00435DAA 6A00            push 00000000


* Reference To: USER32.MessageBeep, Ord:0000h
:00435DAC E80B1C0900      Call 004C79BC
:00435DB1 68E9AD4C00      push 004CADE9
:00435DB6 6A00            push 00000000
:00435DB8 6A0C            push 0000000C

//Le (C) indique que c'est un saut conditionnel
//On nous indique aussi sa provenance (a gauche du (c)), à savoir : 00435D09.
//Faites 'Goto Code Location' et tapez 00435D09.
//W32dasm nous emmène ici :

* Reference To: USER32.SendDlgItemMessageA, Ord:0000h
:00435CF3 E8181D0900      Call 004C7A10
:00435CF8 68235F4D00      push 004D5F23
:00435CFD 683C5B4D00      push 004D5B3C
:00435D02 E871C50500      call 00492278
:00435D07 85C0            test eax, eax
:00435D09 0F859B000000    jne 00435DAA

//(le JNE nous envoie sur "Sorry, your ...." quand le code est faux...)

* Possible StringData Ref from Data Obj ->"mirc.ini.
:00435D0F 687CCF4C00      push 004CCF7C

* Possible StringData Ref from Data Obj ->"oryx"
:00435D14 68E3AD4C00      push 004CADE3

* Possible StringData Ref from Data Obj ->"show"
:00435D19 68DDAD4C00      push 004CADDD


* Possible StringData Ref from Data Obj ->"about"
:00435D1E 68D6AD4C00      push 004CADD6
:00435D23 E8D8600200      call 0045BE00
:00435D28 BE105E4E00      mov esi, 004E5E10
:00435D2D BF3C5B4D00      mov edi, 004D5B3C
:00435D32 33C0            xor eax, eax
:00435D34 83C9FF          or ecx, FFFFFFFF
:00435D37 F2              repnz
:00435D38 AE              scasb
:00435D39 F7D1            not ecx
:00435D3B 2BF9            sub edi, ecx
:00435D3D 87F7            xchg edi, esi
:00435D3F 8BC7            mov eax, edi
```

```
:00435D41 8BD1            mov edx, ecx
:00435D43 C1E902          shr ecx, 02
:00435D46 F3              repz
:00435D47 A5              movsd
:00435D48 8BCA            mov ecx, edx
:00435D4A 83E103          and ecx, 00000003
:00435D4D F3              repz
:00435D4E A4              movsb
:00435D4F 68235F4D00      push 004D5F23
:00435D54 683C5B4D00      push 004D5B3C
:00435D59 E8F6C70500      call 00492554
:00435D5E 6A00            push 00000000


* Possible Ref to Menu: MenuID_0017, Item: "Register..."
* Possible Reference to Dialog: DialogID_0033, CONTROL_ID:0085, ""
:00435D60 6885000000      push 00000085
:00435D65 A1C0204E00      mov eax, dword ptr [004E20C0]
:00435D6A 50              push eax


* Reference To: USER32.DeleteMenu, Ord:0000h (ici il appelle la fonction qui efface
'Register' du menu)
:00435D6B E8541A0900      Call 004C77C4
:00435D70 6A01            push 00000001
:00435D72 8B5508          mov edx, dword ptr [ebp+08]
:00435D75 52              push edx


* Reference To: USER32.EndDialog, Ord:0000h
:00435D76 E89D1A0900      Call 004C7818


* Possible Reference to Dialog: DialogID_0040
:00435D7B 6A40            push 00000040
:00435D7D 6A00            push 00000000


* Possible Reference to String Resource ID=01912: "mIRC Registration!"
:00435D7F 6878070000      push 00000778
:00435D84 E87748FDFF      call 0040A600
:00435D89 50              push eax
:00435D8A 6A00            push 00000000


* Possible Reference to String Resource ID=01911:
"Your registration has been entered successfully...Thanks for."
:00435D8C 6877070000      push 00000777
:00435D91 E86A48FDFF      call 0040A600
:00435D96 50              push eax
:00435D97 8B4D08          mov ecx, dword ptr [ebp+08]
:00435D9A 51              push ecx
```

-> Donc si on change le 'jne 00435DAA' en 'je 00435DAA' le programme ira sur *"Your registration has been entered successfully..."* uniquement quand le code sera faux.

Il faut donc changer 'jne 00435DAA' en 'je 00435DAA' donc 0F859B000000 devient 0F849B000000 (OF85xxxxxx devient OF84xxxxxx, et inversemment...cf MemenTo 1)

-> On clique sur la ligne 00435D09 pour savoir quel offset modifier (en effet dans la barre du bas, W32dasm nous indique l'offset ou on se trouve).

-> Ensuite prenez un éditeur héxadécimal, allez à l'offset et modifier 2.exe comme indiqué précedemment.

-> Sauvegardez, et relancer le programme et essayez de vous enregistrez, rentrez un nom et un serial bidon.

Bravo, mIRC et enregistré on constate également que 'Register' ne figure plus dans le menu 'Help'. En plus, votre nom apparait dans 'About' !! Quittez mIRC et relancez le programme et là.... oh surprise, le programme n'est plus enregistré :(Et oui...comme la plupart des programmes mIRC effectue une vérification du nom/serial au démarrage.

On réfléchit et on se souvient que lorsque on c'est enregistré le menu '*Register*' avait disparu.On cherche alors dans 'Ref Menu' la reference 'Register' et on le trouve !. On sait également que pour supprimer un menu le programme doit faire appel à la fonction **USER.DELETEMENU**. On recherche donc un endroit ou on trouve une référence au menu 'Register' **et** à la commande User.deletemenu.

-> Cliquez donc plusieurs fois sur 'Register' jusqu'à ce que vous trouviez 'Register' et un peu plus haut la commande qui permet de supprimer le menu. On la trouve, et cela nous donne cela :

```
:004923EA 681F024D00      push 004D021F
:004923EF 8B4C240C        mov ecx, dword ptr [esp+0C]
:004923F3 51              push ecx


* Reference To: ADVAPI32.RegQueryValueA, Ord:0000h

:004923F4 E8CB4E0300      Call 004C72C4
:004923F9 85C0            test eax, eax
:004923FB 7565            jne 00492462
:004923FD 6A02            push 00000002
:004923FF 68235F4D00      push 004D5F23
:00492404 E867B1FAFF      call 0043D570
:00492409 68235F4D00      push 004D5F23
:0049240E 55              push ebp
:0049240F E864FEFFFF      call 00492278
:00492414 85C0            test eax, eax
:00492416 754A            jne 00492462     //voilà quelque chose qui nous intéresse...
                                           //(détermine si le menu est affiché ou non)
:00492418 8B0424          mov eax, dword ptr [esp]
:0049241B 50              push eax
```

```
* Reference To: ADVAPI32.RegCloseKey, Ord:0000h

:0049241C E88B4E0300     Call 004C72AC
:00492421 6A00           push 00000000


* Possible Ref to Menu: MenuID_0017, Item: "Register..."
//(Voilà la référence qui nous intéresse...)

* Possible Reference to Dialog: DialogID_0033, CONTROL_ID:0085, ""

:00492423 6885000000     push 00000085
:00492428 8B15C0204E00   mov edx, dword ptr [004E20C0]
:0049242E 52             push edx


* Reference To: USER32.DeleteMenu, Ord:0000h
//(Et la commande permettant de supprimer le menu 'Register...').
```

La comme avant, il suffit de changer un je en jne donc jne 00492462 devient je 00492462 en héxadécimal 744A devient 754A

Voilà, comme avant notez l'offset à modifier et allez les changer avec l'éditeur hexadécimal winhex.exe, sauvegardez, relancez le mIRC. Puis rentrez une nom et un serial bidon, comme avant le programme vous dis "Thank...", quitter mIRC, relancez le et là bravo, mIRC est complètement cracké, en effet notre nom et dans 'About' et 'Register' n'est plus là.

[Conclusion :] C'était pas trop dur, mIRC est un petit programme facile à cracker, mais cela permet au moins d'acquérir un peu de pratique.

Nombre de visites depuis le 15/02/2003