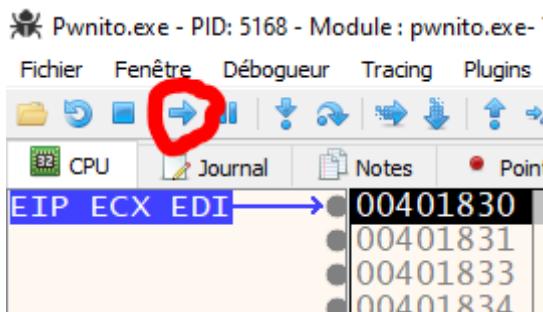


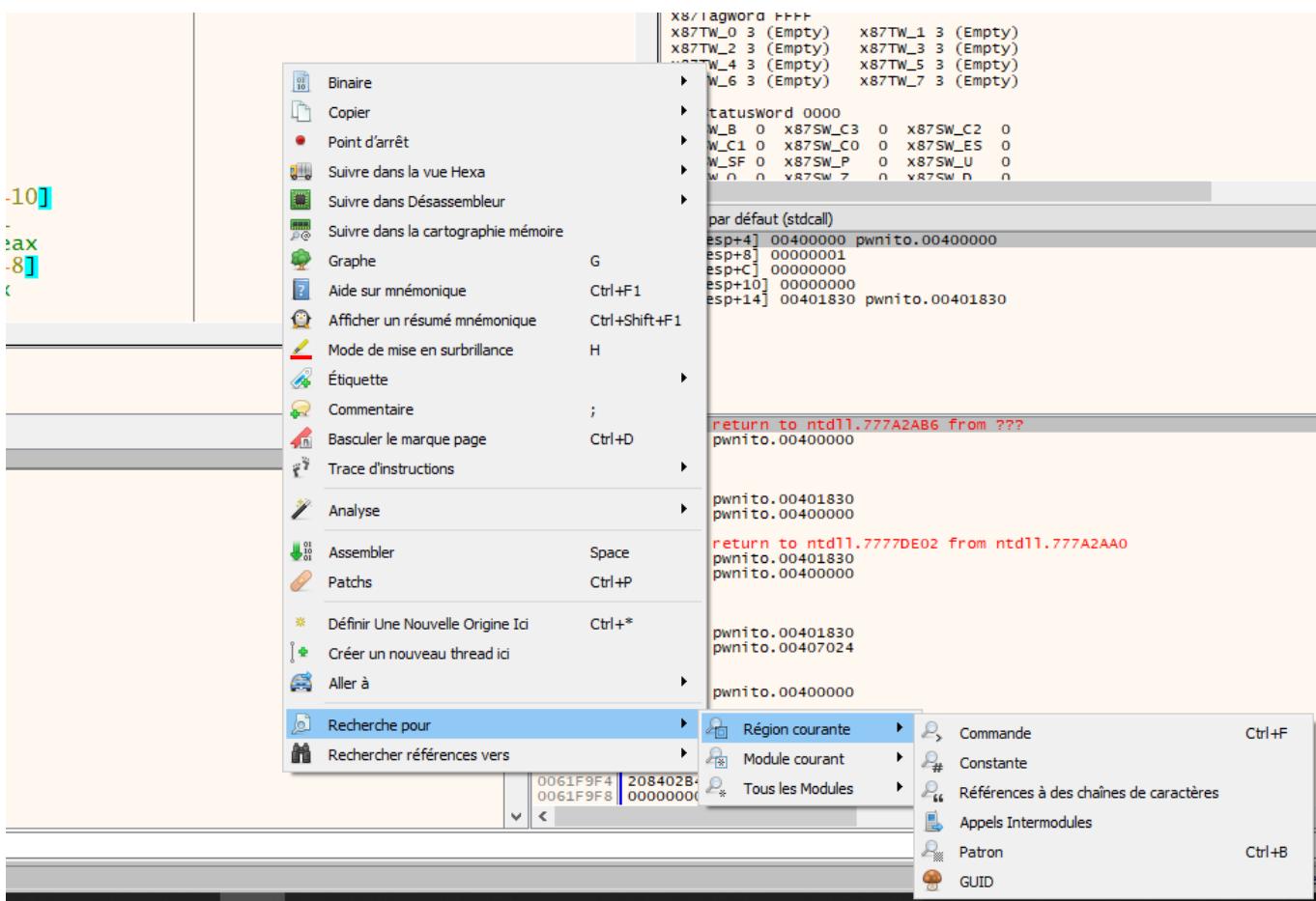
[PWN]

PWNITO Writeup

On avance le debugger d'un cran pour aller au début du programme :



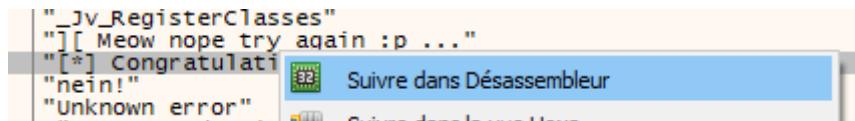
Rechercher pour → Région courante → Références à des chaînes de caractères :



"Congratulation" nous intéresse :

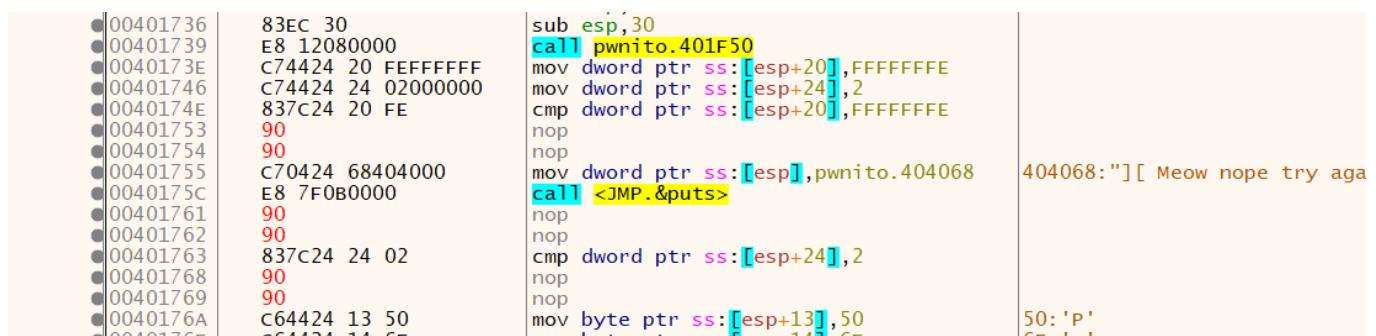
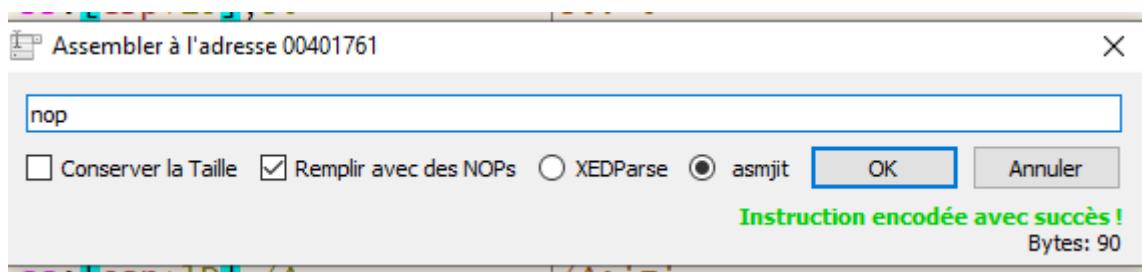
```
"libgcj_s.dll"
"_Jv_RegisterClasses"
"]][ Meow nope try again :p ..."
"[*] Congratulations"
"nein!"
"Unknown error"
"An attempt domain access (domain)"
```

Clique droit suivre dans désassembleur :



```
"_Jv_RegisterClasses"
"]][ Meow nope try again :p ..."
"[*] Congratulations
"nein!"
"Unknown error"
```

On remplit les fonctions pour sauter la formation du tableau avec des instructions "nop" :



00401736	83EC 30	sub esp,30	
00401739	E8 12080000	call pwnito.401F50	
0040173E	C74424 20 FFFFFFFF	mov dword ptr ss:[esp+20],FFFFFFFE	
00401746	C74424 24 02000000	mov dword ptr ss:[esp+24],2	
0040174E	837C24 20 FE	cmp dword ptr ss:[esp+20],FFFFFFFE	
00401753	90	nop	
00401754	90	nop	
00401755	C70424 68404000	mov dword ptr ss:[esp],pwnito.404068	404068:"]"[Meow nope try aga
0040175C	E8 7F0B0000	call <JMP.&puts>	
00401761	90	nop	
00401762	90	nop	
00401763	837C24 24 02	cmp dword ptr ss:[esp+24],2	
00401768	90	nop	
00401769	90	nop	
0040176A	C64424 13 50	mov byte ptr ss:[esp+13],50	50:'P'
0040176C	CC C3 00 00	int3	

On fais un patch du fichier

The screenshot shows the Immunity Debugger interface. On the left, the assembly view displays the following code snippet:

```
00401746 C74424 24 02000000 mov dword ptr ss:[esp+24],2
0040174E 837C24 20 FE cmp dword ptr ss:[esp+20],FFFFFFFE
00401753 90 nop
00401754 90 nop
00401755 C70424 68404000 mov dword ptr ss:[esp+24],2
0040175C E8 8F0B0000 call <JMP.&puts>
00401761 90 nop
00401762 90 nop
00401763 837C24 24 02 cmp dword ptr ss:[esp+20],FFFFFFFE
00401768 90 nop
00401769 90 nop
0040176A C64424 13 50 mov byte ptr ss:[esp+24],2
0040176F C64424 14 6F mov byte ptr ss:[esp+20],0
00401774 C64424 15 30 mov byte ptr ss:[esp+24],2
00401779 C64424 16 77 mov byte ptr ss:[esp+20],0
0040177E C64424 17 6E mov byte ptr ss:[esp+24],2
00401783 C64424 18 33 mov byte ptr ss:[esp+20],0
00401788 C64424 19 64 mov byte ptr ss:[esp+24],2
0040178D C64424 1A 5F mov byte ptr ss:[esp+20],0
00401792 C64424 1B 65 mov byte ptr ss:[esp+24],2
00401797 C64424 1C 34 mov byte ptr ss:[esp+20],0
0040179C C64424 1D 7A mov byte ptr ss:[esp+24],2
004017A1 C64424 1E 69 mov byte ptr ss:[esp+20],0
004017A6 C64424 1F 6C mov byte ptr ss:[esp+24],2
004017AB C64424 20 79 mov byte ptr ss:[esp+20],0
004017B0 C70424 86404000 mov dword ptr ss:[esp+24],2
004017B7 E8 340B0000 call <JMP.&puts>
```

A right-click context menu is open over the assembly code at address 00401754, with the option "Appliquer" selected.

The "Patches" dialog box is open, showing a list of applied patches:

- 0|00401753:75->90
- 0|00401754:0E->90
- 1|00401761:EB->90
- 1|00401762:73->90
- 1|00401768:75->90
- 1|00401769:60->90

An information message box says "6/6 patches appliqués!" with an "OK" button.

On ouvre le fichier cracké et on obtient le flag :

The terminal window shows the following output:

```
C:\Users\...> ./pwnito
][ Meow nope try again :p ...
[*] Congratulations
Po0wn3d_e4zily  @Appuyez sur une touche
```

Flag : Po0wn3d_e4zily