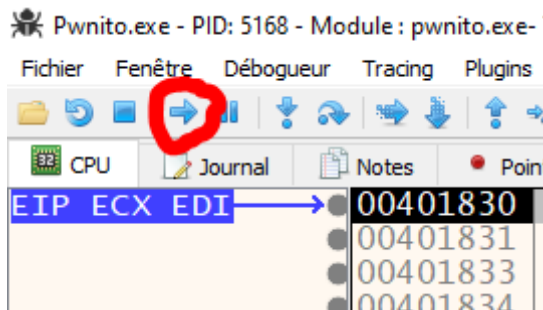


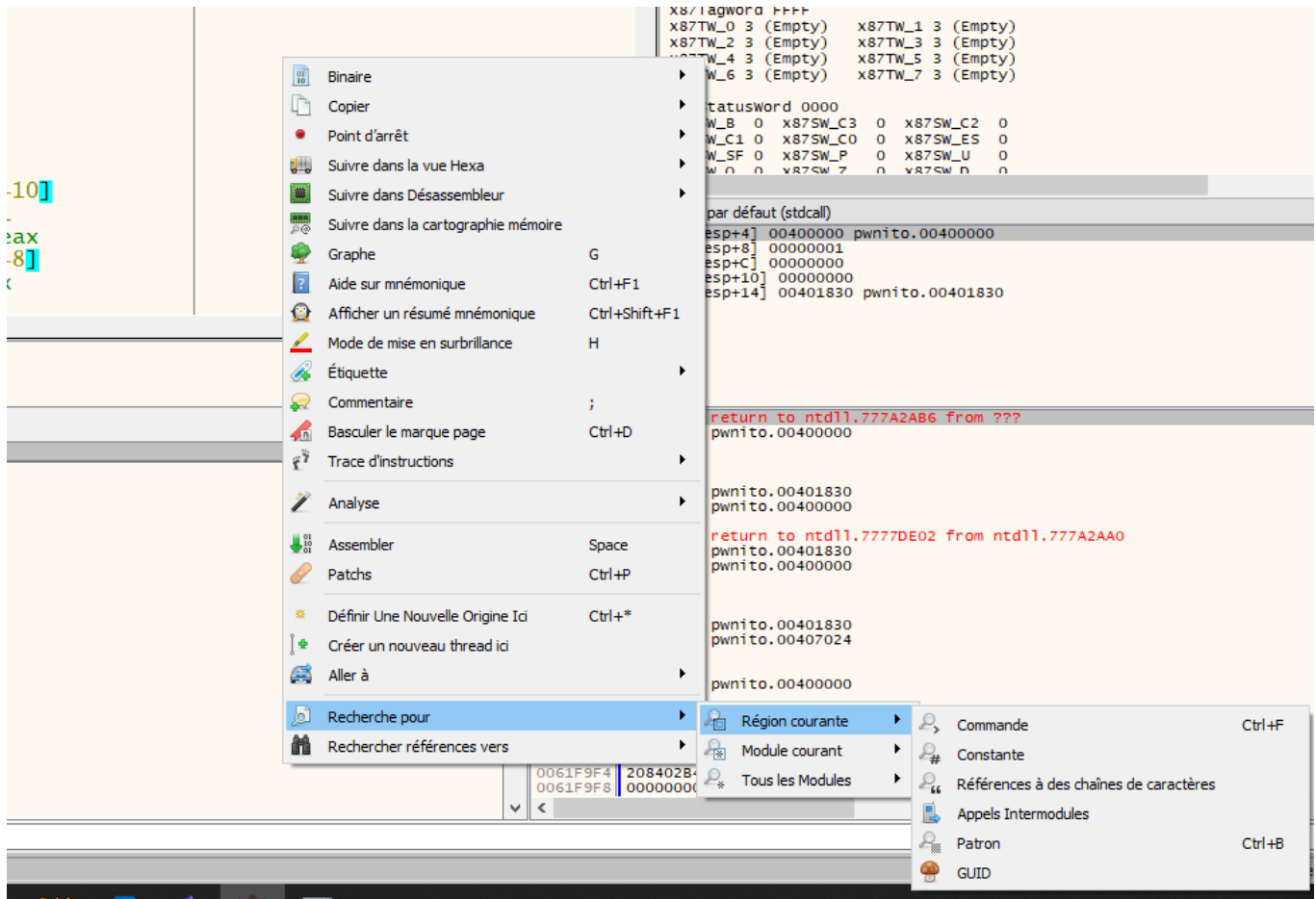
[PWN]

## PWNIT0 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 :

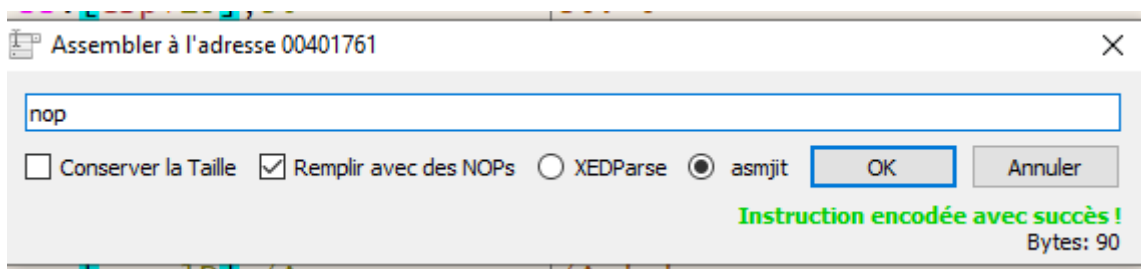
```
"libgcj_s.dll"  
"_Jv_RegisterClasses"  
"[ Meow nope try again :p ..."  
"[*] Congratulation"  
"nein!"  
"Unknown error"  
"Argument déjà existant (FORMAT)"
```

Clique droit suivre dans désassembleur :

```
"_Jv_RegisterClasses"  
"[ Meow nope try again :p ..."  
"[*] Congratulation"  
"nein!"  
"Unknown error"  
"Argument déjà existant (FORMAT)"
```

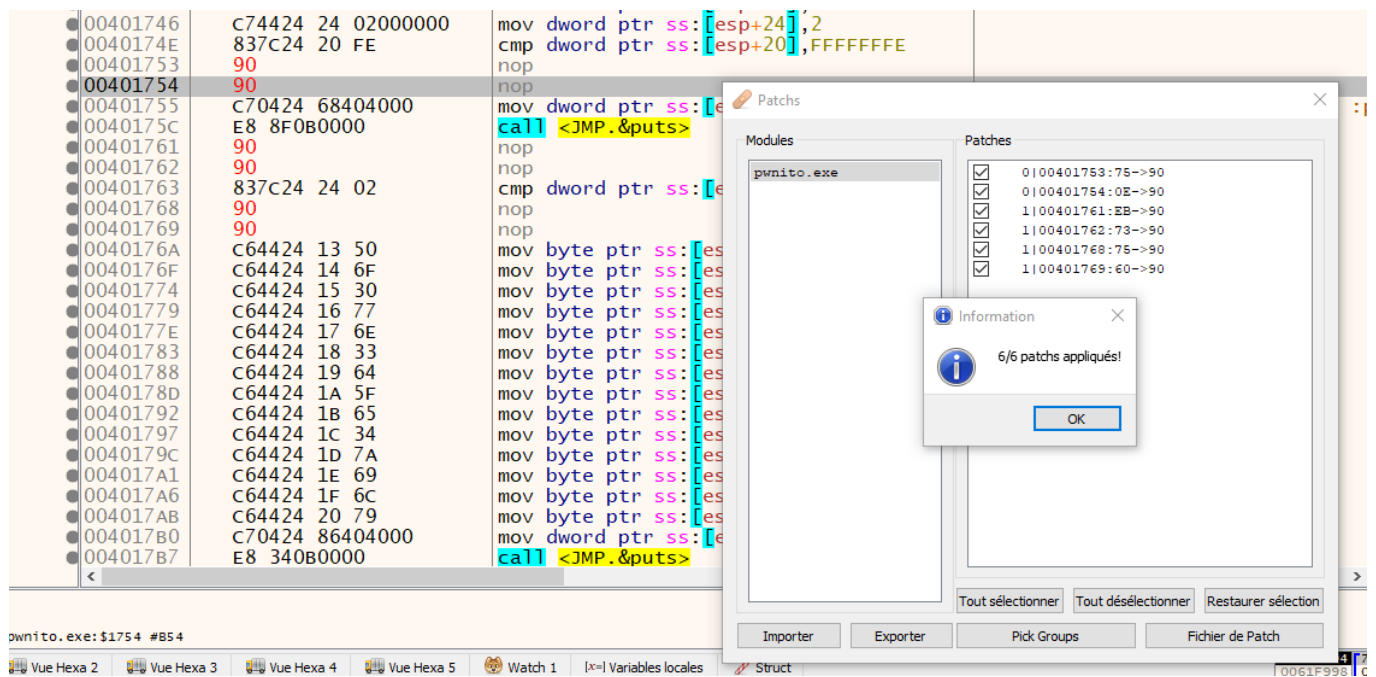
Suivre dans Désassembleur

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

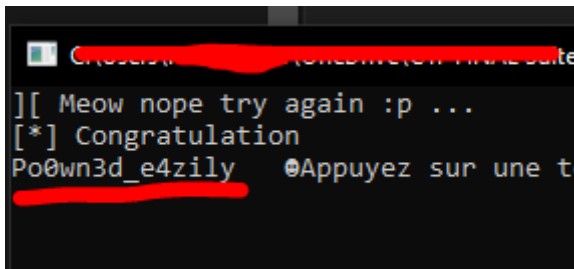


Adresse	Hex	Disassemblé	Commentaire
00401736	83EC 30	sub esp,30	
00401739	E8 12080000	call pwnito.401F50	
0040173E	C74424 20 FFFFFFFF	mov dword ptr ss:[esp+20],FFFFFFFE	
00401746	C74424 24 02000000	mov dword ptr ss:[esp+24],2	
0040174E	837C24 20 FE	cmp dword ptr ss:[esp+20],FFFFFFFE	
00401753	90	nop	
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'

On fais un patch du fichier



On ouvre le fichier cracké et on obtient le flag :



**Flag** : Po0wn3d\_e4zily