

WRITE UP CHALLENGE 'N0pe' - Rédigé par Hugo

1ère étape :

Télécharger le fichier exécutable.

2ème étape :

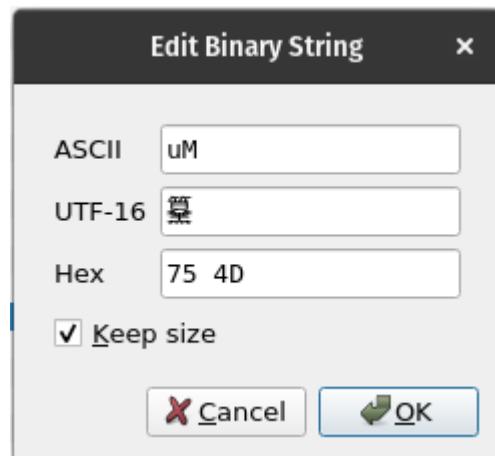
L'exécuter et constater qu'on nous demande un mot de passe (SPOILER : Le mdp ne peut pas être bruteforcé, ou en tout cas, le CTF sera fini lorsqu'il sera bruteforce).

3ème étape :

Ouvrir EDB, insérer le fichier et aller au point de démarrage.

00005635:7aabeb564	e8 d7 fb ff ff	call 0x56357aabeb140	ASCII "Enter the password: "
00005635:7aabeb569	48 8d 05 94 0a 00 00	lea rax, [rel 0x56357aabf004]	
00005635:7aabeb570	48 89 c6	mov rsi, rax	
00005635:7aabeb573	48 8d 05 c6 2a 00 00	lea rax, [rel 0x56357aac1040]	
00005635:7aabeb57a	48 89 c7	mov rdi, rax	
00005635:7aabeb57d	48 8e fb ff ff	call 0x56357aabeb110	
00005635:7aabeb582	48 8d 45 c0	lea rax, [rbp-0x40]	
00005635:7aabeb586	48 89 c6	mov rsi, rax	
00005635:7aabeb589	48 8d 05 d0 2b 00 00	lea rax, [rel 0x56357aac1160]	
00005635:7aabeb590	48 89 c7	mov rdi, rax	
00005635:7aabeb593	e8 98 fb ff ff	call 0x56357aabeb130	
00005635:7aabeb598	48 8b 15 e1 2c 00 00	mov rdx, [rel 0x56357aac1280]	
00005635:7aabeb59f	48 8d 45 c0	lea rax, [rbp-0x40]	
00005635:7aabeb5a3	48 89 d6	mov rsi, rdx	
00005635:7aabeb5a6	48 89 c7	mov rdi, rax	
00005635:7aabeb5a9	e8 10 04 00 00 00	call FACILE!bool std::operator==<char, std::ch...	
00005635:7aabeb5ae	84 c0	test al, al	
00005635:7aabeb5b0	74 28	je 0x56357aabeb5da	

On peut voir sur la capture d'écran ci-dessus, qu'il y a un test "je" qui signifie une comparaison de valeur. On va donc éditer le test pour mettre un non equal to.



4ème étape :

Insérer des points d'arrêts et puis exécuter.

Ci-dessous, c'est les petits points rouges.

● 00005635:7aabeb0	75 4d	jne 0x56357aabeb5ff
● 00005635:7aabeb2	48 8d 45 bf	lea rax, [rbp-0x41]
● 00005635:7aabeb6	48 89 c7	mov rdi, rax
● 00005635:7aabeb9	e8 ac fc ff ff	call FACILE!main::{lambda()#1}::operator()()

5ème étape :

Exécuter le code et regarder l'output :



The screenshot shows the EDB debugger's output window titled "edb output". It contains the following text:
Enter the password: test
Félicitations, voici le flag : NHM2I{jkMOPawBR1-SjwMGEu1EJ-4Z4TNCTzxd}!

Flag : NHM2I{jkMOPawBR1-SjwMGEu1EJ-4Z4TNCTzxd}