C my mind

Razvan

Overview

This challenge implies founding the key and iv for the aes cbc encryption used for encrypting the so file that a has the flag in it.

1 Dumping the encrypted so file

To dump the encrypted so file you need pwndbg to set the breakpoint at main function and from there to run the program untill you see that something is load in memory with dl.Pwndbg will show you the pid and the filedesciptor of the encrypted so file, with which you can dump it with cp /proc/15989/fd/3 /Desktop/cmymind.bin

2 Finding and decrypting the the iv and key for the aes

Looking trough the decompiled compiled code you will see cbc aes so for finding the key and iv you need to look trough the encrypt function there you will see 4 functions and find 8 hex values in every function the first 2 functions contains the encrypted key value and in in the next 2 functions the hex values represent the iv.In the same functions where you find the hex values you will find the encryption algorithms use to encrypt them.In the original code they were called in the same order so your mission is to analyze them and reproduce theme,that part will be pretty easy so here i will show the part that of the algorithm that divide the key and call the function that calls the transpose of the matrix.

[You can find the complete code of the algorithm in the private folder algo.c]

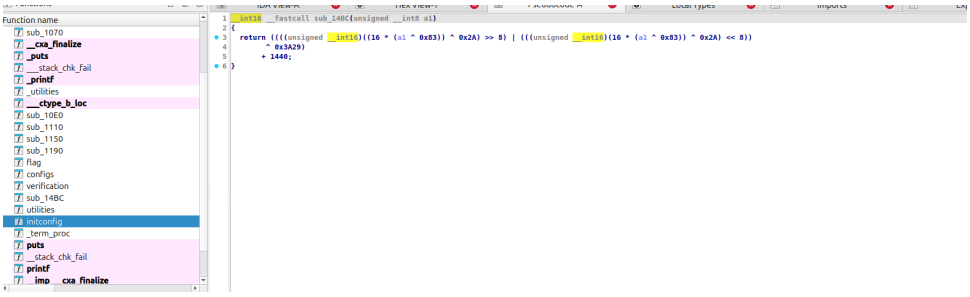
3 Decrypting encrypted so file with aes ”

After you find the key and iv you need to make a function to decrypt the prevoius encrypted file that you obtained.To do this i use but you can use any programming language.

[Full code can be seen in test$_e$.c]

4 Looking trough the so file

łAfter you decrypted the so file you will find half of the falg and an array with hex values to find the last part of the flag you need to find the encryption algorithm with was used to encrypt theme and reverse it. *Example filler text:*



[Full code can be seen in extra.c]

5 UVT{1n_m3mory_w3_trust_wh3n_dysk_1s_ly1ng}