題目:FIFO

丟進 IDA 裡面看

1. 觀察 main,可以看到他在裡面 open 一個 file 並且寫入東西,接著在 execve 這個 file,合理懷疑寫入的是程式碼,並且 execve 這邊是 fork 出來的,很明顯就是另一個 subprocess 的概念。parent 建立了 fifo,並且 call 了 write ,write 東西到這個 fifo 裡面,我們合理懷疑這個就是把 flag 傳過去
2. 在 IDA 中看那個地址上面的東西,可以發現像是亂碼,不像 flag
   所以估計是 child process 接到這個之後還會做一些處理，我們可以從 gdb 設斷點在 open 知道這個 subprocess 的 file 是在/tmp/khodsmeogemgoe , 這個就是我們 subprocess 會運行的程式碼的檔案
3. 用 IDA 去開這個 file,觀察一下會發現,sub_1209 對接收到的文字做了一些操作。
4. gdb fifo
   1. set follow-fork-mode child,讓我們 fork 之後跟隨的是 child,
   2. catch exec : 讓我們可以跟進 exec 後的程式
   3. b*0x0000555555554000 + 0x12f5 : 因為 sub_1209 操作做完會是在這個位置
   4. c
   5. flag 出現了