b06705001 b06705001 楊力行

這次的題目開啟了 NX 因此要用 ROP 或是 ret2libc，同時也開啟了 pie，所以如果要用 ret2libc 需要先 leak 出 base_address。

經過上次的作業我知道了我可控 GOT，只是只能執行一次無法同時 leak 加上執行，而在把 puts 改為指向 casino 函式後就可以進行無限次的修改。

接著，我需要 leak 出 libc 的基址，而在 GOT 的函式中，srand 的 RDI 是可靠著修改 seed 來控制的，因此目標就是他，利用上次的劫持 GOT 的方法將他的動態鍵結改成 printf 的位址並且靠著 name 的 overflow 在 seed 寫入 __libc_main_start 的 GOT 的位址，接著再重回 casino 的頂部執行到這句，利用 recvuntil 接收，再用 u64 解碼後儲存，接著將這位址減掉__libc_main_start 的偏差再加上 system 的偏差，就可以得到 system function 的真實位址

有 system 之後還差/bin/sh 而 name 的地方是可讀可寫，就把/bin//sh 寫入 name，並在其後先加個\x00 在用 A 補滿，接著再用 guess 的 overflow 把 seed 改成指向 name 的位址，接著把 srand 再次改成 system 的位址後，再次呼叫 puts 到 casino 開頭執行 system(/bin//sh)就成功 getshell 了。

在解題的過程中，我的本地系統導致我卡了很久，因為不明的原因它所鍵接的 libc 的偏差值和題目給的 libc.so 完全不同，而當我把同樣的 code 改成 remote 後一次就過了。