Computer Security HW0x7

R08946007 資科所 蔡昀達

Nickname：r08946007

Casino++

1. 跟 casino 不同的地方是想要利用 leak address 的方式找到 syscall 位置
2. 先利用改寫 puts@got 來達到回圈執行 casino 涵式，可以多次寫記憶體
3. 因為 seed 變數可控，因此把 srand@got 改寫成 printf@plt，把 seed 改寫成 libc_start_main@got 來達到 leak
4. Leak 出 base address 之後算出 syscall 位置
5. 把 atoi@got 改寫成 syscall 位置
6. 再下一次 read_int 涵式輸入/bin/sh 成功 get shell
7. FLAG{Y0u_pwned_me_ag4in!_Pwn1ng_n3v3r_di4_!}
8. 過程中 syscall 一直失敗，一直跳到 vprintf，過很久才發現是 link 到本機的 libc，吐血

- objdump –d casino++
  - printf@got, printf@plt
  - puts@got, puts@plt
  - atoi@got, atoi@plt
- objdump –R casino++
  - libc_start_main@got
- readelf –s ./libc.so | grep “libc_start”
  - libc_start_main offset
- readelf –s ./libc.so | grep “system”
  - system offset