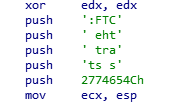
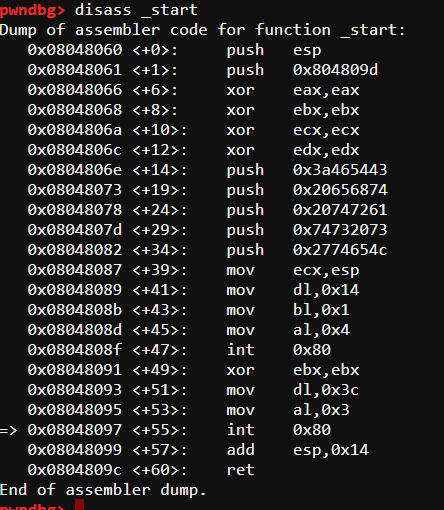
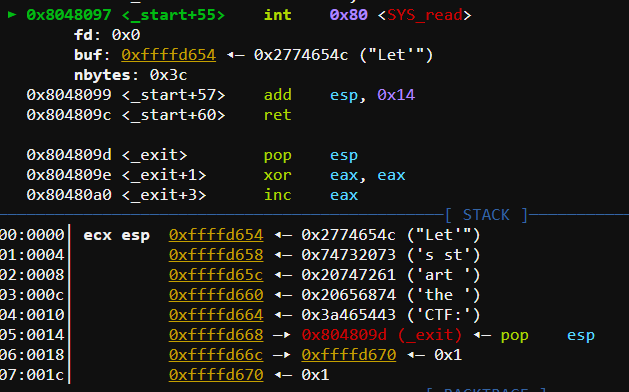


Mở file bằng IDA, chúng ta thấy chương trình có hai hàm, \_exit và \_start. Phân tích xem chương trình làm gì.

Đầu tiên nó sẽ xor các thanh ghi với nhau, sau đó push  chuỗi gì đó vào stack. Tiếp theo nó mov al ,4, rồi int 0x80 để gọi sys\_write in ra chuỗi đó. Sau đó nó mov al, 3 để gọi sys\_read, cho phép nhập vào.

Debug bằng gdb:





Ta thấy nó nhập vào từ địa chỉ 0xffffd654, và return address của nó nằm ở địa chỉ 0xffffd668

Offset = 0xd668 – 0xd654 = 0x14

Vậy ta có thể ghi đè địa chỉ return của chương trình .

Vì chương trình không có gì khác giúp ta lấy flag nên ta có thể dùng shellcode và return về shellcode.

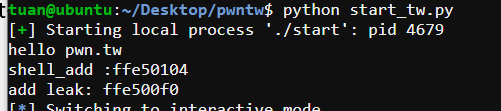
Để return về shellcode thì ta cần biết địa chỉ shellcode nhập vào, mà server luôn bật aslr nên ta cần tìm cách leak địa chỉ để ghi shellcode.

Trong bài này chỉ có hàm sys\_write để in ra dữ liệu gì đó.

Ta để ý ở \_start + 39, chương trình mov ecx, esp. Tức là nếu ta return về hàm sys\_write 1 lần nữa thì ta sẽ in ra được địa chỉ đầu của stack và khi nó chạy đến hàm sys\_read thì nó sẽ nhập địa chỉ esp là địa chỉ chứa dữ liệu nhập vào.

\_start+39 = 0x8048087

Buffer = ‘a’\* 0x14 + p32(\_start+39)



Vị trí nhập dữ liệu ở 0xfffe500f0 , thì địa chỉ return = địa chỉ leak + 0x14.

Địa chỉ shell = địa chỉ leak + 0x14

Buffer2 = ‘a’\*0x14 + shell\_add + shell.