**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

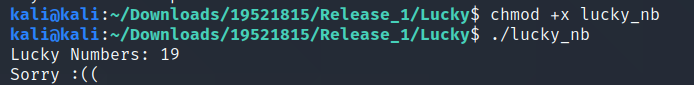
**RE CHALLENGES: LUCKY\_NB**

|  |  |  |  |
| --- | --- | --- | --- |
| **Giảng viên hướng dẫn** | **Phạm Văn Hậu** | | **ĐIỂM** |
| **Sinh viên thực hiện 1** | **Trần Đức Lương** | **19521815** |  |

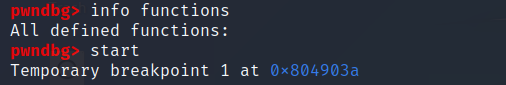
Đây là file ELF 32-bit chạy trên Linux. Tuy nhiên, file này đã bị stripped.

https://raw.githubusercontent.com/ducluongtran9121/RE-WriteUp/main/19521815/Release_1/Lucky/file.png?token=AOZ4VHM66PULRS7ADXEAXEDAUOOZM

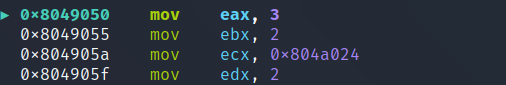
Chạy thử chương trình, nhập vào giá trị 19 thì chương trình báo về kết quả sai “Sorry :((”. Ý tưởng bài này sẽ là nhập vào 1 số, nếu nó là lucky number thì sẽ trả về kết quả thành công.

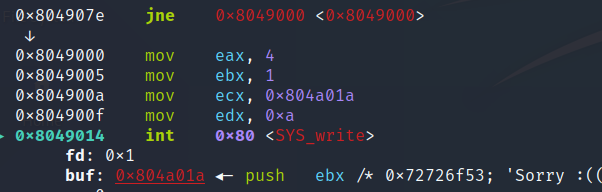


Dùng GDB mở file, ta không tìm thấy functions nào cả vì file đã bị stripped. Khi đó chạy câu lệnh start sẽ debug chương trình từ dòng đầu tiên của chương trình.

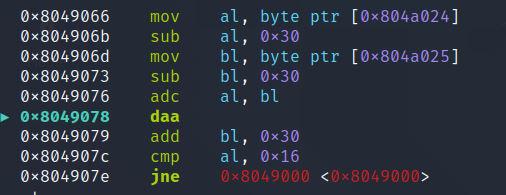


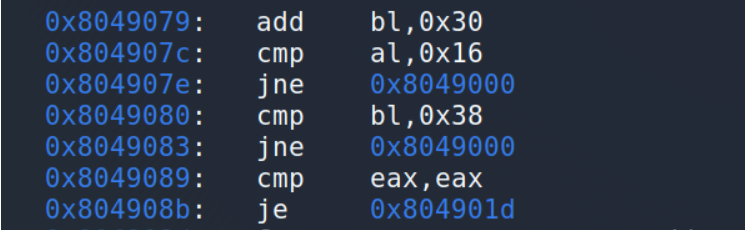
Đây chính là bước nhập chuỗi số, nó sẽ được lưu ở địa chỉ 0x804a024 với tối đa 2 ký tự.





Lần lượt lấy từng kí tự của chuỗi số vừa nhập trừ đi 0x30 lưu tại 2 thanh ghi al và bl ,sau đó thực hiện so sánh tổng hai giá trị trên với 0x16 (1). Nếu bằng chương trình tiếp tục so sánh kí tự thứ 2 (lúc đầu) với 0x38, ngược lại nhảy xuống hàm tại 0x8049000 báo sai.



Nếu kí tự thứ 2 chính bằng 0x38(2), tức là ‘8’ (theo Ascii code), chương trình nhảy xuống hàm tại offset 0x804901d, chính là hàm báo thành công. 

Kết hợp (1) và (2) suy ra hai kí tự đều bằng 0x38 tức là ‘8’. Khi đó lucky number chính là “88”

