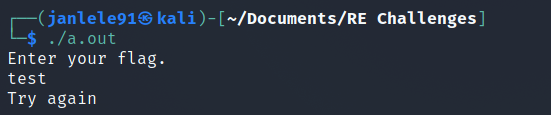
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

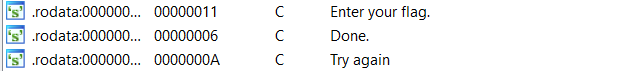
**RE CHALLENGES 2: Just crackme**

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

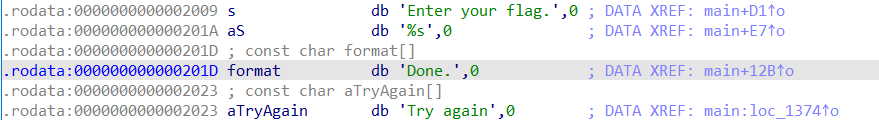
File **a.out** là một file thực thi ELF 64-bit. Thực hiện chạy thử file trên kali linux với flag “**test**” thì cho ra dòng “**Try again”.** Ý tưởng của bài này là đi tìm flag thích hợp, giống như việc đi tìm password ở các bài trước.



Thực hiện mở IDA Pro bản 64-bit thực hiện quá trình dịch ngược. Thực hiện xem strings có trong file thì thấy có các dòng dưới . “**Done.**” chính là mục tiêu chúng ta cần hướng đến.



Truy vết các strings trên thì thấy nó đều nằm trong hàm **main**.



Mở hàm main có trong IDA Pro:



Chương trình yêu cầu nhập vào chuỗi **v7** rồi yêu cầu so sánh với chuỗi **v6**, nếu **bằng nhau** thì đó chính là flag ta cần tìm. Phân tích code thì thấy chuỗi v6 chính bằng **chuỗi s nối với chuỗi src**, cụ thể **v6** = “**Wait, your name is USER**”. Vậy flag ở đây là “**Wait, your name is USER**”, thực thi chương trình với chuỗi này ta thấy chương trình báo “**Done.**” thành công.

