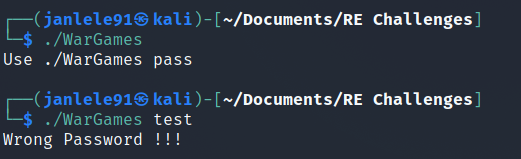
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

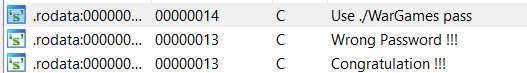
**RE CHALLENGES 2: WARGAMES**

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

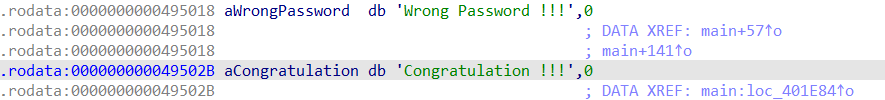
Đây là file thực thi ELF 64-bit. Thực hiện chạy thử chương trình với không tham số đầu vào thì thấy chương trình báo cần thêm pass. Sau đó thử chạy với pass = “**test**” thì chương trình báo “**Wrong Password !!!**”. Ý tưởng của bài này chỉ là tìm password thích hợp.



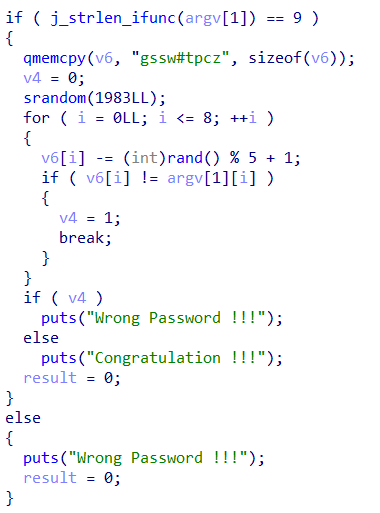
Mở file **Wargames** bằng IDA Pro để thực hiện quá trình dịch ngược. Xem subview strings thì thấy có dòng “**Congratulation !!!**” chính là mục tiêu chúng ta cần hướng đến.



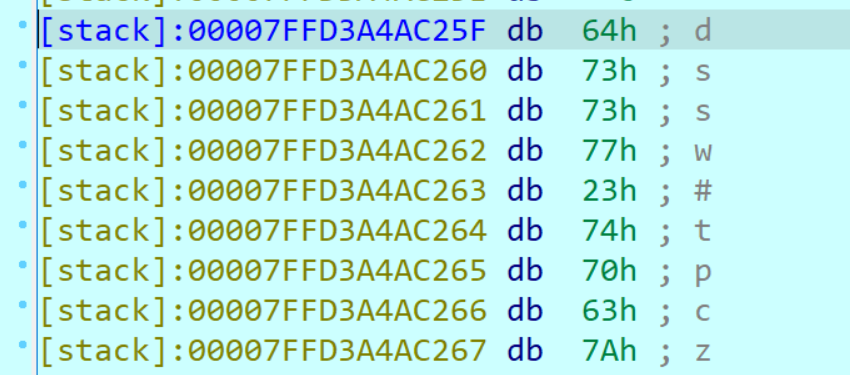
Truy vết string trên thì thấy nó nằm trong hàm **main**.



Mở hàm **main**, bắt đầu phân tích:



Ở đây **argv[1]** **chính là pass** **chúng ta nhập**, dựa vào dòng if đầu tiên ta thấy pass nhập vào phải là một chuỗi có **9 ký tự**. Để đi đến “**Congratulation !!!**”, chúng ta phải so sánh **argv[1]** với **v6**, nếu bằng nhau thì thành công. Tuy nhiên, với giá trị ban đầu là “**gssw#tpcz**”, qua vòng for thì từng kí tự của **v6** bị biến đổi bởi hàm **rand()**. Vì là random nên chúng ta phải đi debug chương trình 9 lần tương ứng với 9 kí tự để xem giá trị của từng kí tự sau khi rand() là bao nhiêu. Thực hiện debug với **Remote Linux Debugger** lần 1 với pass là “**abcd12345**” như hình dưới.



Quan sát ta thấy sau lần **rand()** đầu tiên thì **v6[0] = ‘d’ (0x64)** mà **argv[1][0] = ‘a’** (pass là “abcd12345”) nên chương trình in ra “**Wrong Password !!!**”. Vậy để tiếp tục debug lần 2 thì **argv[1][0]** lúc này phải bằng ‘**d**’, ta sẽ debug với pass “**dbcd12345**”. Quá trình diễn ra tương tự cho từng kí tự, kết quả cuối cùng ta nhận được là “**dont play**”. Vậy đây chính là password chúng ta cần tìm.

