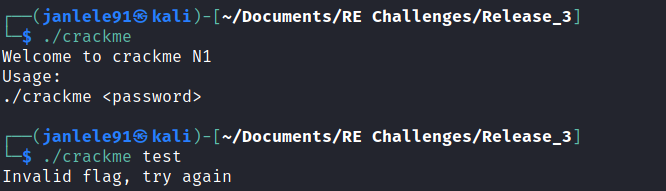
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

**RE CHALLENGES 3: Catalina**

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

Đây là file thực thi PE 64-bit. Có thể thấy chương trình yêu cầu nhập password như là tham số đầu vào. Thực hiện chạy thử với password “***test***” thì thấy chương trình báo flag không hợp lệ.

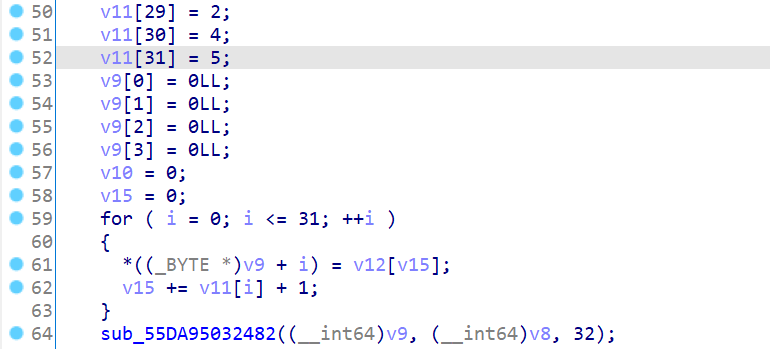


Mở file ***crackme*** bằng IDA Pro thực hiện quá trình dịch ngược. Mở Subview -> Strings thì thấy xuất hiện dòng chữ “***Congratulations…***” chính là mục tiêu chúng ta cần hướng đến.

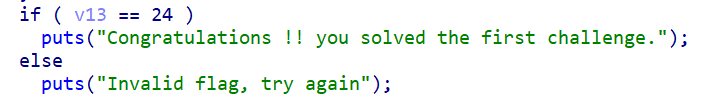


Thực hiện truy xuất strings trên thì thấy nó nằm trong hàm ***main***. Bắt đầu phân tích hàm ***main***:

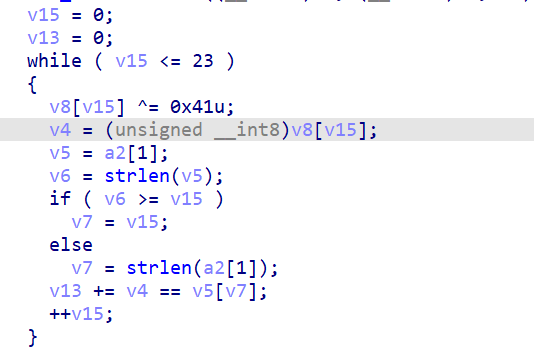




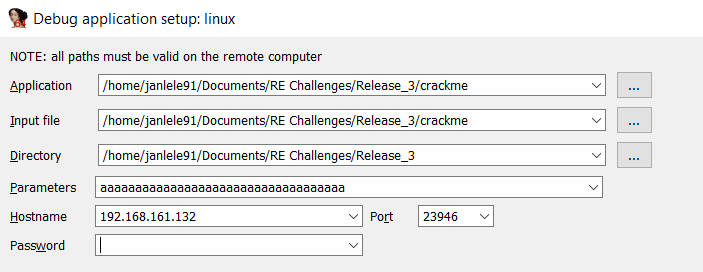
Chương trình thực hiện tạo giá trị ***v8*** từ ***v12*** cho trước thông qua ***v9***. Ta không cần quan tâm phần này vì không liên quan đến password chúng ta nhập vào.



Có thể nhìn thấy rằng, chương trình sẽ chỉ in ra dòng chữ thành công khi giá trị ***v13 == 24***.



Giá trị ***v13 == 24*** khi và chỉ khi ***v4 == v5[v7]*** trong cả 24 lần lặp của vòng while. Cụ thể ***v5 = a2[1]*** chính là giá trị password chúng ta nhập vào. Cứ mỗi lần lặp, chương trình lấy từng kí tự của ***v8*** sau khi ***xor*** với ***0x41*** gán vào ***v4*** và so sánh với kí tự ở vị trí tương ứng của password ***v5***. Nếu bằng nhau thì giá trị ***v13*** tăng thêm 1. Điều này có nghĩa là password ***v5*** cần tìm sẽ có tối thiểu 24 kí tự và chứa chuỗi 24 kí tự đầu tiên chính bằng ***v8*** sau khi vòng while kết thúc.



Thực hiện Linux remote debug với password đầu vào như trên tại breakpoint ngay sau vòng while vừa rồi, thì thấy giá trị của chuỗi v8 tại đó là “***flag{2020\_sana\_sa3ida:)}***”



Vậy password cần tìm là bắt đầu bằng 24 kí tự trên. Thực hiện chạy với password = “***flag{2020\_sana\_sa3ida:)}***” hay “***flag{2020\_sana\_sa3ida:)}aa***” hay “***flag{2020\_sana\_sa3ida:)}aaaaa***” đều thành công.

