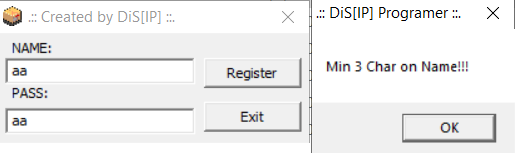
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

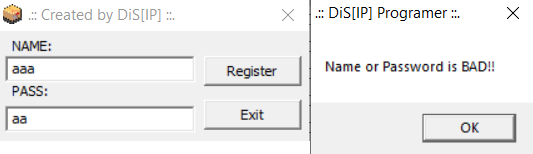
**RE CHALLENGES: CRACK001**

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

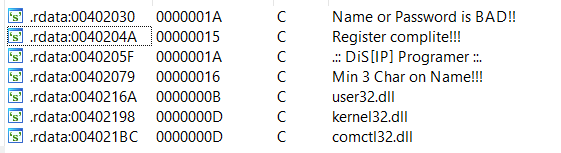
Chạy thử chương trình trên nền tảng Window, giao diện của chương trình bao gồm phần NAME và PASS. Thử test với cặp (NAME,PASS) là (aa, aa) thì chương trình báo “Min 3 Char on Name!!!” tức là phần NAME phải là chuỗi có ít nhất 3 kí tự.



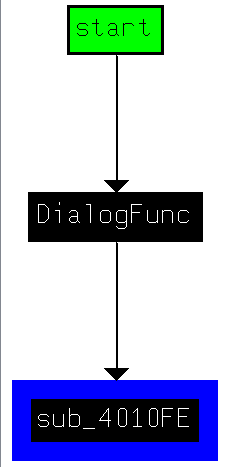
Thử test với cặp (aaa, aa) thì chương trình báo “Name or Password is BAD!!” . Từ đó có thể hiểu được rằng ý tưởng của bài này là nhập Name có ít nhất 3 kí tự và phần Password có thể phụ thuộc vào name.



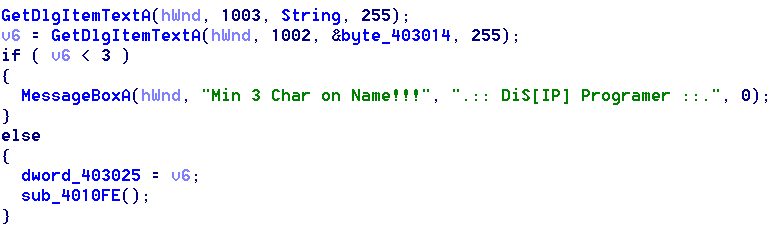
Phân tích chương trình bằng IDA Pro, mở phần strings lên thì thấy “Register complite” chính là câu thông báo nhập name và password thành công.



Dưới đây là sơ đồ hoạt động của chương trình với 3 hàm.



Dưới đây là mã giả của hàm DialogFunc. Có thể dựa vào phân tích đầu Write-up để xác định được byte\_403014 lưu Name và String sẽ lưu Password. Nếu thảo mãn điều kiện nhiều hơn 2 kí tự của Name, chương trình sẽ tiếp tục gọi hàm sub\_4010FE().



Chương trình tại đây sẽ lặp qua hết tất cả ký tự của Name. Dựa vào kiểm tra ô nhớ của Name ta thấy nó có tối đa 5 kí tự.(1)

Nếu thỏa mãn 1 trong 3 điều kiện if đầu tiên kết hợp với LOBYTE(v1) = v1 + 1 ở dưới nên nếu Name có kí tự thứ i là ‘z’ hay ‘Z’ hay ‘9’ thì kí tự của Password thứ 2\*i tương ứng vẫn sẽ là ‘z’ hoặc ‘Z’ hoặc ‘9’. Còn nếu không thỏa mãn 3 điều kiện đó thì kí tự thứ 2\*i của Password sẽ bằng kí tự thứ i của Name + 1. Bên cạnh đó, sau mỗi lần lặp HIBYTE(v1) += v0++ +97 nên kí tự thứ 2\*i + 1 của Password sẽ chạy từ ‘a’ đến ‘e’ do i < 5 (do (1)). Ví dụ nếu Name là “aaa” thì Password sẽ là “babbbc”.



Ở đây em sẽ nhập Name là “zZ9” thì dựa theo phân tích trên password sẽ là “zaZb9c”. Bài này sẽ có nhiều đáp án và nên nhớ là Name chỉ có tối đa 5 kí tự và tối thiểu 3 kí tự.

