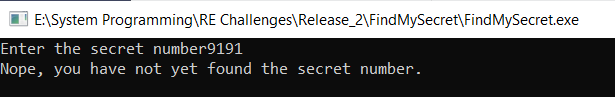
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

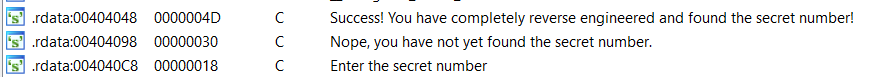
**RE CHALLENGES 2: FindMySecret**

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

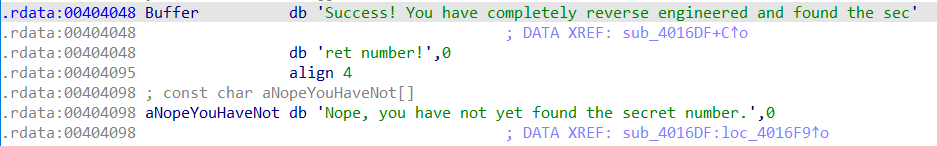
Đây là file exe PE 32-bit. Chạy thử chương trình với secret number “**9191**” thì chương trình báo sai. Nhiệm vụ của chúng ta là đi tìm secret number thỏa mãn.



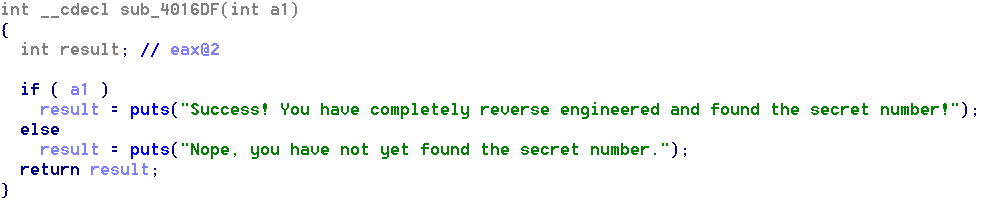
Mở file bằng IDA Pro, mở subview strings thì thấy dòng “**Success! You have completely reverse engineered and found secret number!**” chính là mục tiêu chúng ta cần hướng đến.



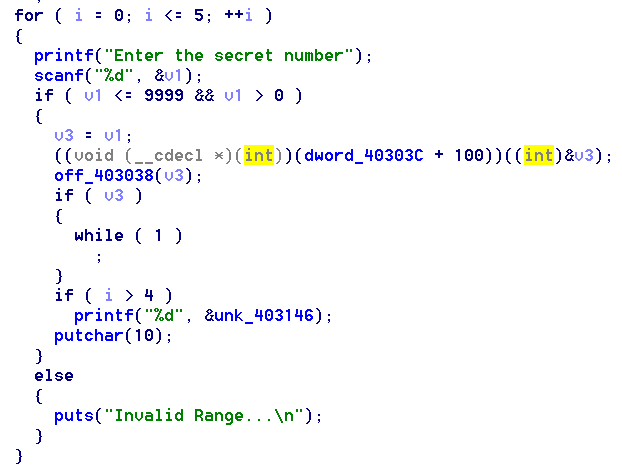
Truy vết các strings trên thì thấy nó nằm ở hàm **sub\_4016DF** trong khi nơi nhập **secret number** nằm ở hàm **start**.



Hàm **sub\_4016DF** cho thấy để in ra dòng thành công “**Success! …**”, giá trị **a1** phải bằng **1**. **(\*)**



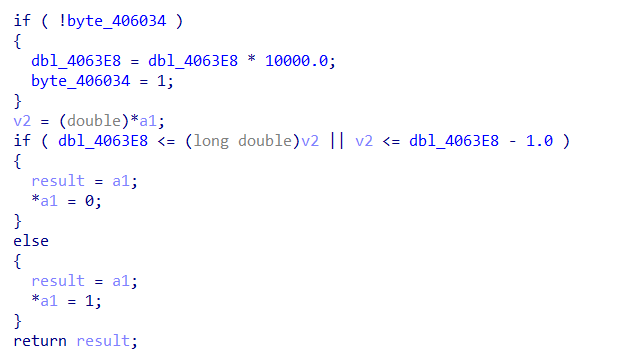
Hình dưới là hàm start, **v1** là nơi lưu secret number chúng ta nhập vào. Giá trị **v1** phải nằm trong đoạn từ 1 đến 9999.



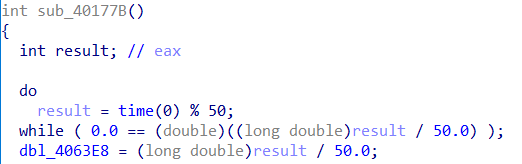


Ta có **dword\_40303C + 100** bằng **0x401708** nên chương trình gọi hàm **sub\_401708(v3)** (v3 = v1).

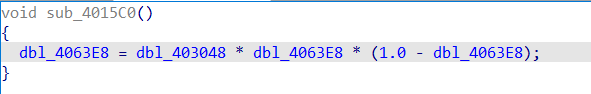
Hàm **sub\_401708** (hình dưới) thực hiện so sánh giá trị **a1** với **dbl\_4063E8**. Kết hợp với **(\*)**, ta suy ra secret number nhập vào phải thỏa mãn **dbl\_4063E8 – 1 < secret number < dbl\_4063E8** . Ta sẽ đi kiểm tra giá trị **dbl\_4063E8**.



Tại hàm **sub\_40177B**, **dbl\_4063E8** được tính dựa trên thời gian thực nhờ vào **time(0).**

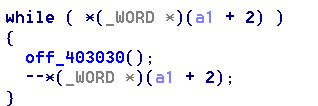


Sau đó tại hàm **sub\_4015C0**, **dbl\_4063E8** được tính bằng công thức như hình dưới trong đó **dbl\_403048 == 3.8**



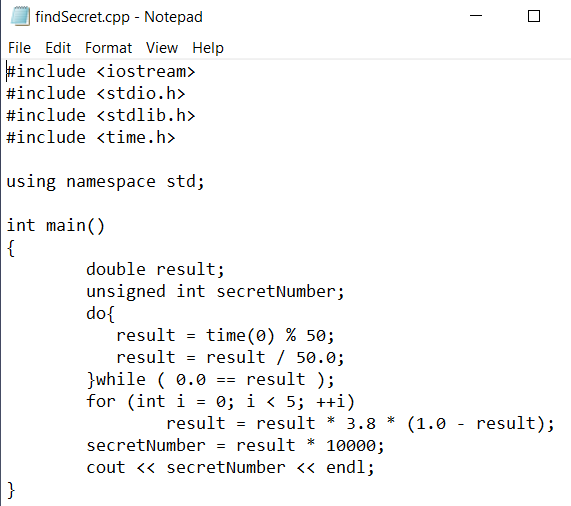


Có thể debug và nhận biết được phép tính trên được thực hiện **5** lần nhờ vào đoạn code bên dưới (**offset\_403030** chính là **sub\_4015C0**)





Từ những nhân xét trên, ta có thể rút ra kết luận là chúng ta không thể chỉ nhập số vào thì sẽ thành công được vì chương trình chạy theo **thời gian thực** và số thỏa mãn cũng thay đổi theo thời gian. Giải pháp ở đây là chúng ta sẽ viết một đoạn code tính số secret thỏa mãn dựa vào thời điểm mình thực thi, rồi in ra kết quả làm đầu vào cho chương trình **FindMySecret.exe**.



Hình trên là đoạn code dùng cho việc tìm ra secret number tại thời điểm thực thi. Compile chương trình bằng g++ cho ra file thực thi **findSecret.exe**, sau đó thực hiện chạy **findSecret.exe** cùng lúc với **FindMySecret.exe** để làm đầu vào. Có thể thấy chương trình đã chạy thành công!

