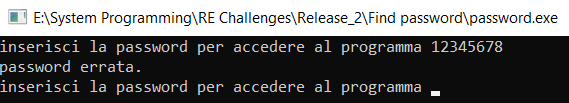
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

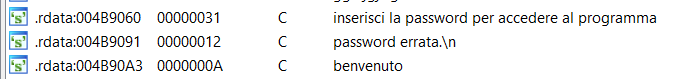
**RE CHALLENGES 2: Find Password**

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

Đây là file exe PE 32-bit. Thử chạy chương trình với password nhập vào là **12345678** thì chương trình báo sai “**password errata.**”. Ý tưởng của bài này cũng là đi tìm password đúng để chạy chương trình thành công.



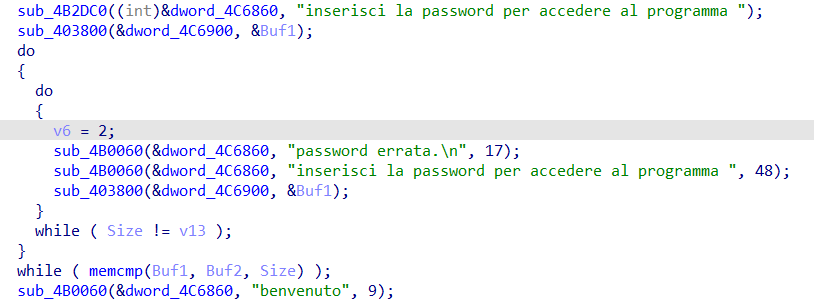
Mở file bằng IDA Pro, mở subview strings thì để ý thấy dòng “**benvenuto**” là mục tiêu chúng ta cần hướng đến.



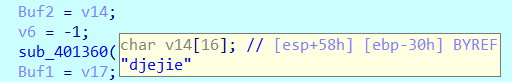
Truy vết string thì thấy nó nằm ở trong hàm **main**.

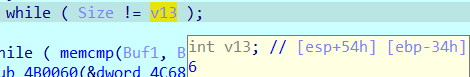


Thực hiện mở hàm **main** và phân tích code.



Cụ thể biến **Buf1** sẽ lưu giá trị password chúng ta nhập vào, trong khi đó bằng quá trình debug thì thấy **Buf2 == “djejie”** và biến **v13 == 6** ( bằng **strlen(Buf2)** ), biến **Size = strlen(Buf1)**.





Thực hiện phân tích thì thấy để chương trình in ra “**benvenuto**” thì **memcmp(Buf1, Buf2, Size) == 0** và **Size == v13** tức là **Size == 6**. Khi đó chúng ta cần nhập password dài 6 kí tự và chính bằng **Buf2** là “**djejie**”.Tuy nhiên, chương trình luôn báo sai ở lần nhập đầu tiên vì hàm **do while(Size != v13)** luôn bắt đầu bằng “**password errata**”. Do đó ta sẽ kiểm tra tính đúng sai ở lần nhập tiếp theo. Thực hiện nhập password bằng “**djejie**” ở lần tiếp theo thì chương trình báo “**benvenuto**” tức là thành công.

