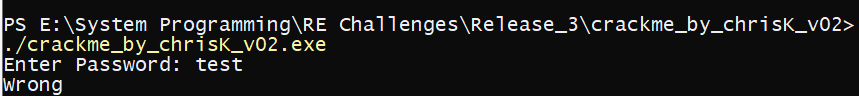
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

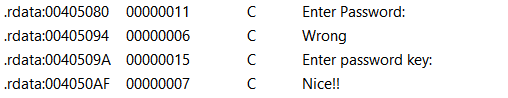
**RE CHALLENGES 3: crackme\_by\_chrisK\_v02**

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

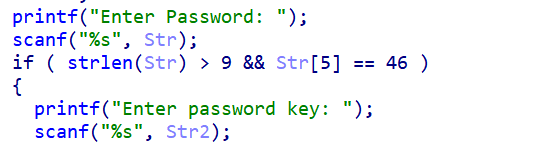
Đây là file exe PE 32-bit. Thử chạy chương trình với password nhập vào là “*test*” thì chương trình báo sai “*Wrong*”. Ý tưởng của bài này cũng là đi tìm password đúng để chạy chương trình thành công.



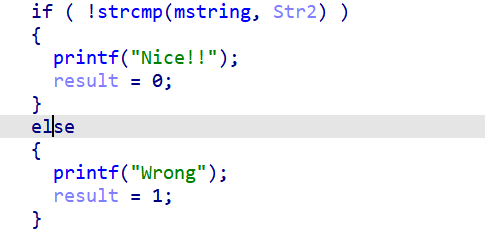
Phân tích file bằng IDA Pro, mở Subview Strings thì thấy xuất hiện dòng ‘*Nice!!*’ chính là mục tiêu chúng ta cần hướng tới. Thực truy xuất thì thấy nó nằm trong hàm ***main***.



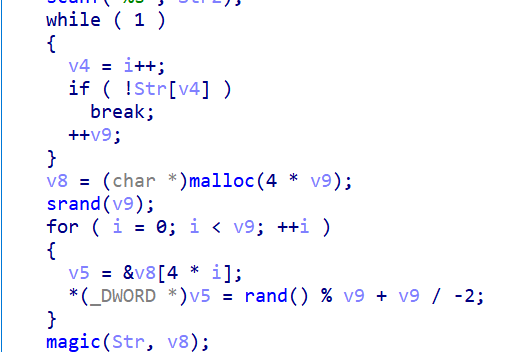
Thực hiện phân tích hàm ***main***, cụ thể password nhập vào sẽ được lưu vào chuỗi ***Str***, nó phải thỏa mãn có nhiều hơn 9 kí tự và kí tự thứ 6 phải là ‘.’ (dấu chấm). Sau đó chương trình yêu cầu nhập password key được lưu vào chuỗi ***Str2***.



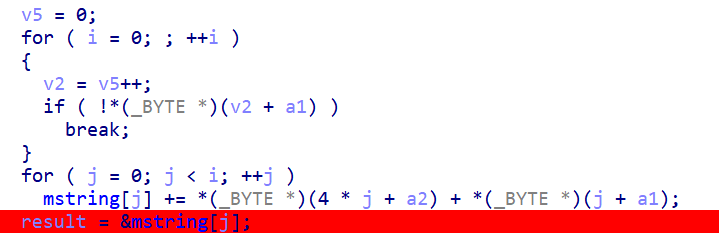
Để chương trình in ra “Nice!!” , chúng ta cần nhập ***Str2*** đúng bằng ***mstring***. Ta sẽ đi tìm giá trị của chuỗi ***mstring***.



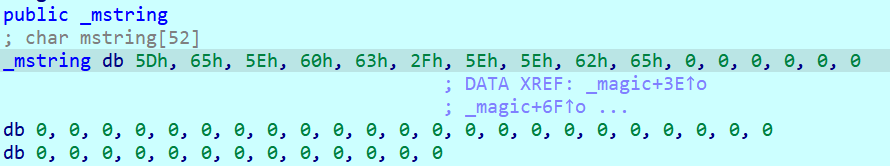
Ở block code này chương trình thực hiện tạo ra chuỗi v8, ta sẽ không cần quan tâm, chỉ cần debug để biết được giá trị v8. Sau đó ***v8*** và ***Str*** được đưa vào làm đối số cho hàm ***magic***.



Trong hàm ***magic***, chương trình thực hiện gán giá trị cho chuỗi ***mstring*** từ chuỗi ***Str*** và ***v8***.Ta chỉ cần đặt breakpoint như hình dưới rồi chạy debug với ***Str = “aaaaa.aaaa”*** để xem chuỗi ***mstring***.



Sau khi debug thành công thì thấy giá trị của mảng ***mstring*** chính bằng chuỗi ***“]e^`c/^^be***”.



Như vậy ta chỉ cần nhập thêm password key ***Str2 = ““]e^`c/^^be”*** với password ***Str = “aaaaa.aaaa”*** thì chương trình sẽ thành công.

