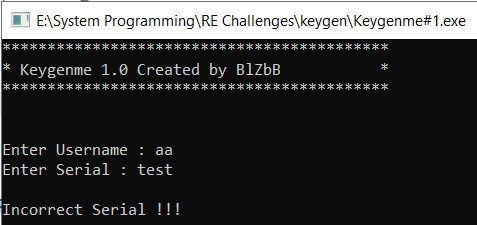
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

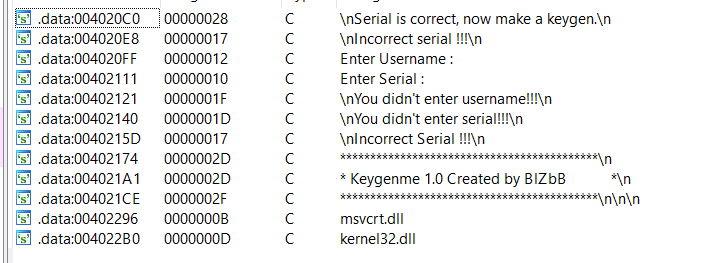
**RE CHALLENGES: KEYGEN**

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

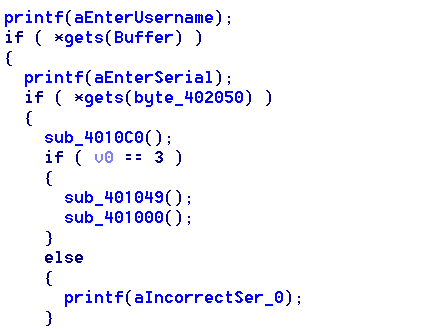
Chạy thử chương trình ta thấy chương trình yêu cầu nhập username và serial. Ý tưởng bài này vẫn là nhập serial phụ thuộc vào username.



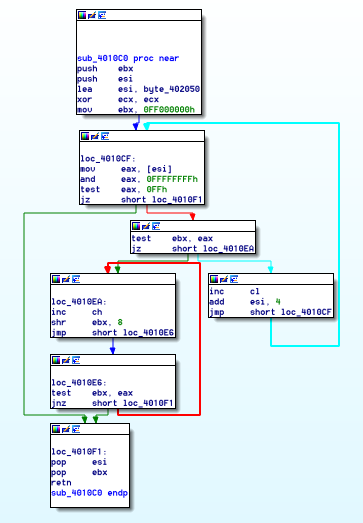
Dùng IDA Pro phân tích file Keygenme#1.exe, mở strings lên sẽ có những câu lệnh mà chương trình trả về, đáng chú ý là cần phải tìm ra username và serial đúng thì chương trình sẽ trả về “Serial is correct, now make a keygen”.



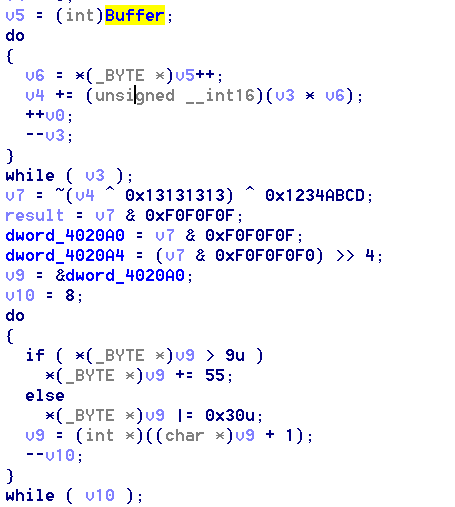
Bắt đầu phân tích bằng mã giả, chương trình bắt buộc yêu cầu nhập username và serial rồi lần lượt lưu vào Buffer và byte\_402050. Chương trình gọi hàm sub\_4010C0() với mong muốn trả về giá trị tại thanh ghi ecx sẽ bằng 3 (do v0 đang được lưu tại thanh ghi ecx).



Sơ đồ hoạt động của hàm sub\_4010C0. Có thể thấy sẽ có 1 vòng lặp tại block 2. Có 2 câu lệnh sẽ tác động đến giá trị của thanh ghi ecx, đó là inc cl và inc ch. Tuy nhiên nếu [ecx] = 3 thì cần có 3 vòng lặp đi qua câu lệnh inc cl và không đi qua inc ch. Khi đó chuỗi serial lưu tại byte\_402050 cần có 12 ký tự, cứ mỗi vòng lặp sẽ lấy từng nhóm 4 ký tự để kiểm tra điều kiện. Cụ thể, mỗi kí tự đầu và kí tự cuối của mỗi nhóm 4 ký tự đó phải đồng thời khác 0. (VD: “aaaabbbbcccc” hoặc “0aaa0aaa0aaa”).



Sau khi chương trình hoàn thành hàm sub\_4010C0 và thỏa mãn [ecx] = 3 thì chương trình tiếp tục gọi hàm sub\_401049() trước và hàm sub\_401000() sau. Để ý ở hàm sub\_401000() sẽ sử dụng hai biến dword\_4020A0 và dword\_4020A4 ở hàm trước là sub\_401049() nên thay vì đọc code ta sẽ chạy debug với username là “aa” để xem giá trị của 2 biến đó sau khi qua hàm sub\_401049().

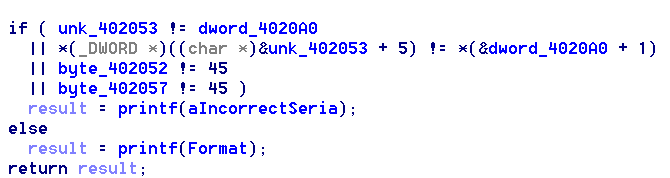


Sau khi chạy hàm sub\_401049() kiểm tra giá trị của 2 biến dword\_4020A0 và dword\_4020A4 được lưu dưới dạng Little Endian.

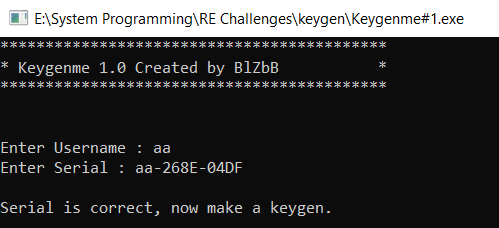
https://lh3.googleusercontent.com/yrA5k2QMpdYsygTn8FspI1PqLVqG1y3rDYW7NVMwbnYIxXgHkxYEcxlcQIdNIHtWVedk2MMP3XfodImxopsiIbtiROEg3h6_eBAFuM9Lm9850n26ngv5UQQD5hbXAu-_EbyQVFO_

Hàm sub\_401000() dưới đây sẽ trả về kết quả dựa trên câu lệnh if. Để thành công ta cần đi vào câu lệnh else, tức là: (serial lưu ở byte\_402050)

* unk\_402053 == dword\_4020A0, tức là 4 kí tự kể từ ví trị thứ 4 của serial sẽ lần lượt bằng 0x32,0x36,0x38,0x45 hay theo ASCII sẽ được chuỗi “268E”
* Điều kiện tiếp theo tương đương với: là 4 kí tự kể từ ví trị thứ 9 của serial sẽ lần lượt bằng 0x30,0x34,0x44,0x46 hay theo ASCII sẽ được chuỗi “04DF”
* Kí tự thứ 3 và thứ 8 của serial sẽ là ‘-’
* Hai kí tự đầu tiên sẽ là bất kỳ.



Vậy với username là “aa” thì serial thích hợp là “aa-268E-04DF”.



Bài này sẽ có nhiều đáp án phụ thuộc vào username. Trên đây chỉ là 1 ví dụ.