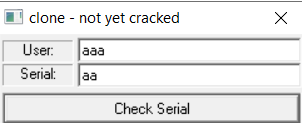
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

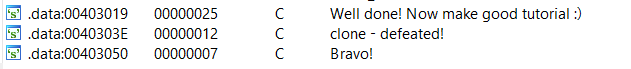
**RE CHALLENGES: CLONE**

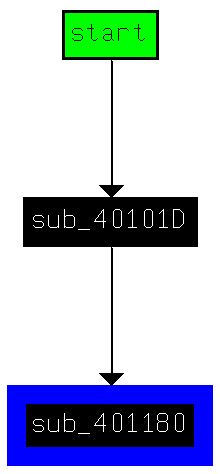
|  |  |  |  |
| --- | --- | --- | --- |
| **Giảng viên hướng dẫn** | **Phạm Văn Hậu** | | **ĐIỂM** |
| **Sinh viên thực hiện 1** | **Trần Đức Lương** | **19521815** |  |

Thử chạy chương trình cho ra một giao diện đăng nhập với user và serial. Thử test như hình dưới thì thấy chương trình không thông báo gì, tức là đã không thành công.

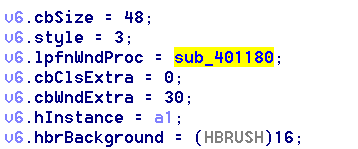


Mở chương trình bằng IDA Pro, dùng strings thì thấy đây là những dòng thông báo thành công, tức là khi mình nhập đúng thì sẽ hiện ra những dòng này. Ý tưởng của bài có lẽ sẽ nhập user và serial sẽ phụ thuộc vào giá trị của user đó.

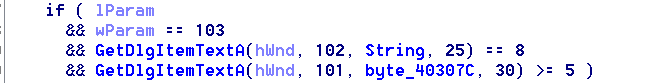


Đây là sơ đồ thực thi của chương trình với hàm start bắt đầu và gọi hàm sub\_40101D().

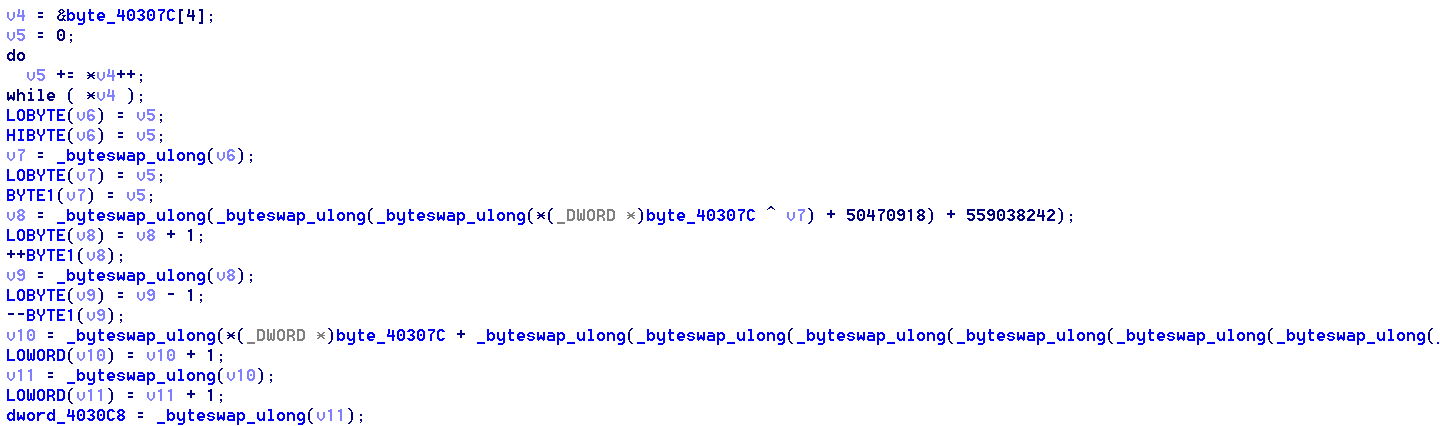
Thực hiện quá trình xem mã giả của hàm sub\_40101D() thì thấy ngay đầu hàm chương trình đã tiếp tục gọi hàm sub\_401180().



Trong hàm sub\_401180() xuất hiện dòng if bên dưới. Sau khi debug thì thấy byte\_40307C chính là biến lưu user và String là biến lưu serial. Cụ thể user phải có số kí tự ít nhất là 5 và serial có đúng 8 kí tự.



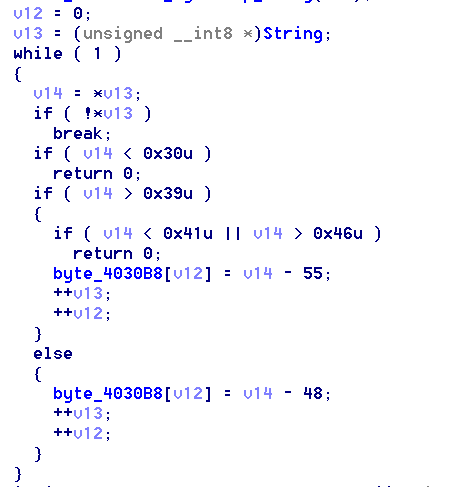
Block code dưới nằm trong hàm sub\_401180() nhằm xử lý thông tin từ user. Cái mình cần quan tâm ở đây là giá trị của biến dword\_4030C8 sau khi chạy xong block này vì dword\_4030C8 sẽ được dùng cho quá trình tiếp theo.



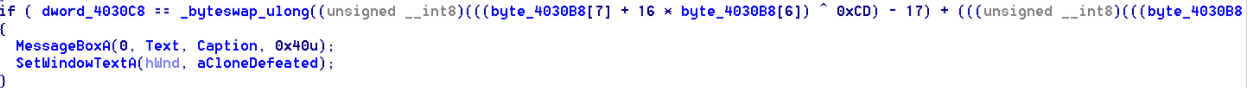
Sau khi debug với user = “11111” thì nhận được dword\_4030C8 = 0x514081B1 (Little Endian)

https://lh4.googleusercontent.com/HNM2jDtvbqGthabTLjiPn2juU5qk5Xb3De8XQop0b7W-Cy7UAdrvYdyDPHhIxroBUY9SpiAqWZc3yuU1OLqlVwHbRMEvp6zj6-0zWhu0VwMDjKGpaJ7VM04i-BelJDIOS7FUhAO2

Bên dưới đây là block xử lí thông tin từ serial, cụ thể hàm này chỉ rõ ra các ký tự của serial chỉ nằm trong dãy các kí tự là (‘0’,’1’,’2’,’3’,’4’,’5’,’6’,’7’,’8’,’9’,’A’,’B’,’C’,’D’,’E’,’F’). Và hơn nữa byte\_4030B8 bây giờ sẽ là một mảng lưu mã hex thật của các ký tự trong khoảng trên. VD chuỗi là “ABC12345” thì byte\_4030B8 = {0xA,0xB,0xC,0x1,0x2,0x3,0x4,0x5}



Dòng if này chính là điều kiện chúng ta cần check, nếu đúng thì chương trình sẽ báo thành công.



Đại loại của dòng if trên sẽ là so sánh xem giá trị tính toán dựa trên byte\_4030B8 có bằng với dword\_4030C8 không. Như phân tích trên dùng với user = “11111” nên ta có: dword\_4030C8 = 0x514081B1 (Little Endian).

Cụ thể khi đó: (s chính là byte\_4030B8)

s[i] thuộc {0x0,0x1,0x2,0x3,0x4,0x5,0x6,0x7,0x8,0x9,0xA,0xB,0xC,0xD,0xE,0xF}

* (s[1] + s[0] << 4) ^ 0x12) + 0x34 = 0xB1 => (s[1] + s[0] << 4) = 0x6F => s[0] == 0x6 ('6') , s[1] ==0xF ('F')
* (s[3] + s[2] << 4) ^ 0x56) + 0x78 = 0x81 => (s[3] + s[2] << 4) = 0x5F => s[2] == 0x5 ('5') , s[3] ==0xF ('F')
* (s[5] + s[4] << 4) ^ 0x90) + 0xAB = 0x40 => (s[5] + s[4] << 4) = 0x05 => s[4] == 0x0 ('0') , s[5] ==0x5 ('5')
* (s[7] + s[6] << 4) ^ 0xCD) + 0xEF = 0x51 => (s[7] + s[6] << 4) = 0xAF => s[6] == 0xA ('A') , s[7] ==0xF ('F')

Suy ra serial cần tìm để dòng if đó đúng là : “6F5F05AF”

Thực hiện đăng nhập với kết quả trên ta nhận được thông báo thành công của chương trình.

