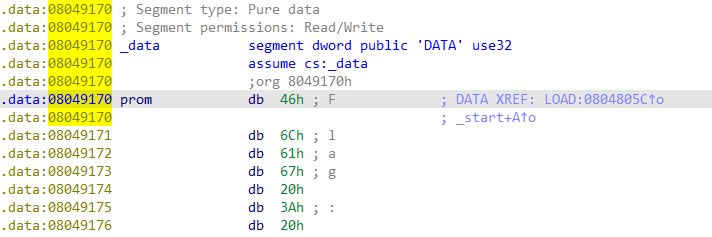
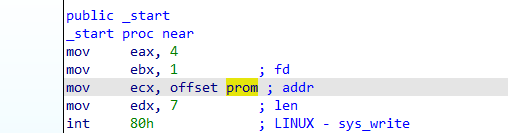
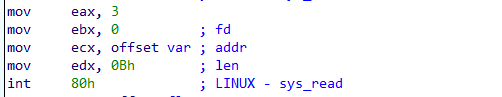
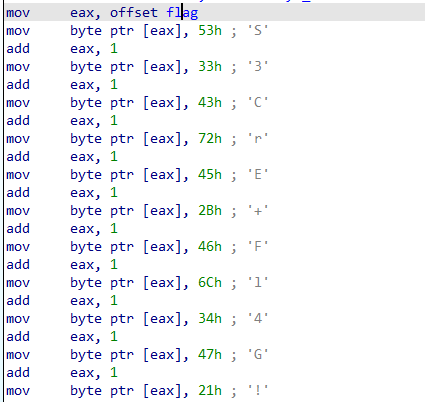
**Bài Crack\_nasm**

Bắt đầu quan sát từ hàm \_start, ta thấy đoạn chương trình trên là hàm thực hiện in ra 7 bytes bắt đầu ở địa chỉ prom để yêu cầu người dùng nhập Flag. 

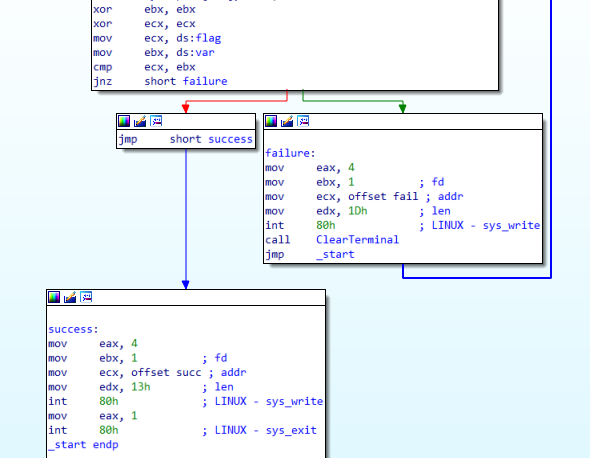
Tiếp theo, chương trình thực hiện đoạn code bên dưới để đọc input vào và lưu ở địa chỉ var.

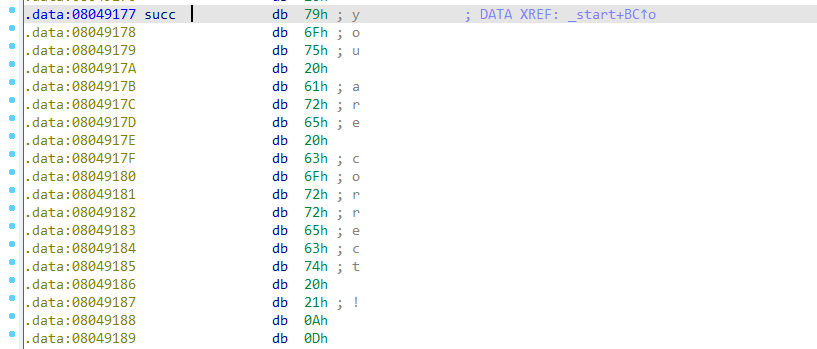
Tiếp theo chương trình gán địa chỉ flag vào thanh ghi eax, sau đó lần lượt gán các giá trị ‘S’, ’3’, ’C’, ‘r’, ‘E’, ‘+’, ‘F’, ‘l’, ‘4’, ‘G’, ‘!’ vào [eax], [eax+1], …, [eax+10], cũng tức là gán ‘S3CrE+Fl4G!’ vào vùng nhớ bắt đầu tại địa chỉ flag.

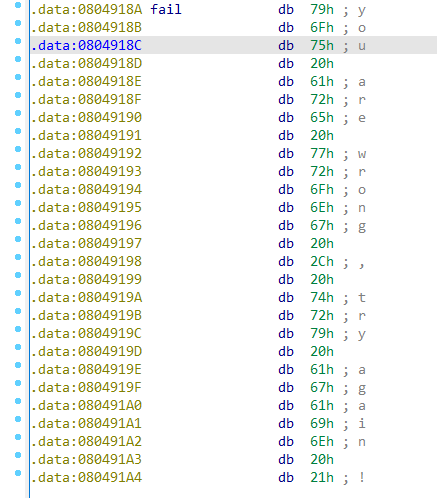


Tiếp theo giá trị tại địa chỉ flag được lưu vào ecx, giá trị người dùng nhập tại var được lưu vào ebx.

Chương trình so sánh ecx và ebx nếu khác nhau in ra giá trị tại địa chỉ fail, ngược lại in giá trị tại địa chỉ success. Vì vậy ta cần nhập flag là S3CrE+Fl4G!







Kiểm tra lại

