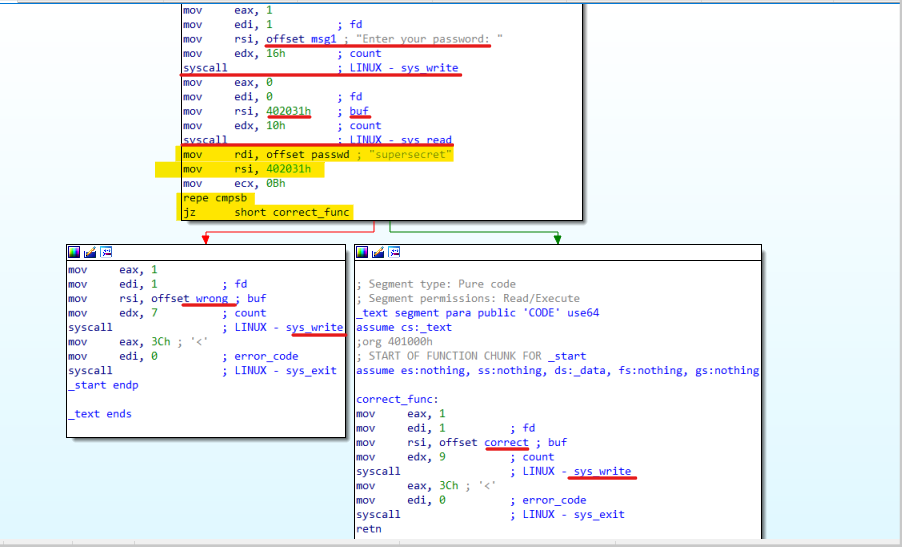
**Nasm**

Chương trình khá đơn giản ta sẽ phân tích tĩnh. Ta thấy chương trình cho người dùng nhâp vào password và lưu ở địa chỉ 402031h, gán rdi bằng địa chỉ paswd (giá trị tại địa chỉ này là chuỗi supersecret), gán địa chỉ 402031h cho rsi, gán ecx bằng 0Bh (giá trị thâp phân là 11 bằng độ dài chuỗi supersecret).

Lệnh cmpsb so sánh byte tại địa chỉ cặp thanh ghi rdi và rsi đang giữ, rsi rdi được tự động tăng sau mỗi lần so sánh(do DF=0), thực chất là so sánh chuỗi supersecret và chuỗi người dùng nhâp.

Chương trình dùng lệnh repe để lặp lại lệnh cmpsb khi cx<>0 và ZF=1 (tức khi kí tự tương ứng của hai chuỗi còn bằng nhau và còn chưa duyệt hết chuỗi). Nếu bằng in ra thông báo correct.

****Vậy chuỗi ta cần nhập là supersecret

Kiểm tra

