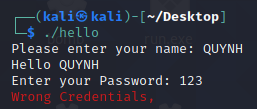
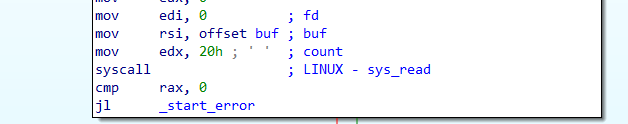
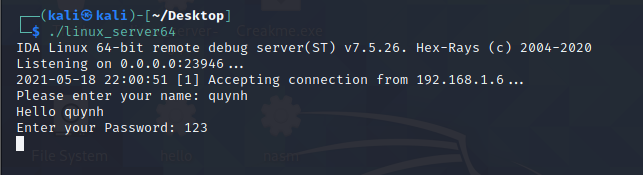
**Hello**

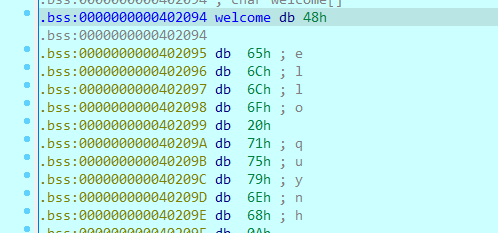
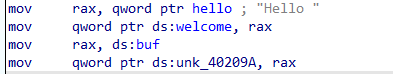
Chạy thử chương trình:



Đọc code assembly ta thấy chương trình cho người dùng nhập name và lưu name vào vùng nhớ có địa chỉ buf

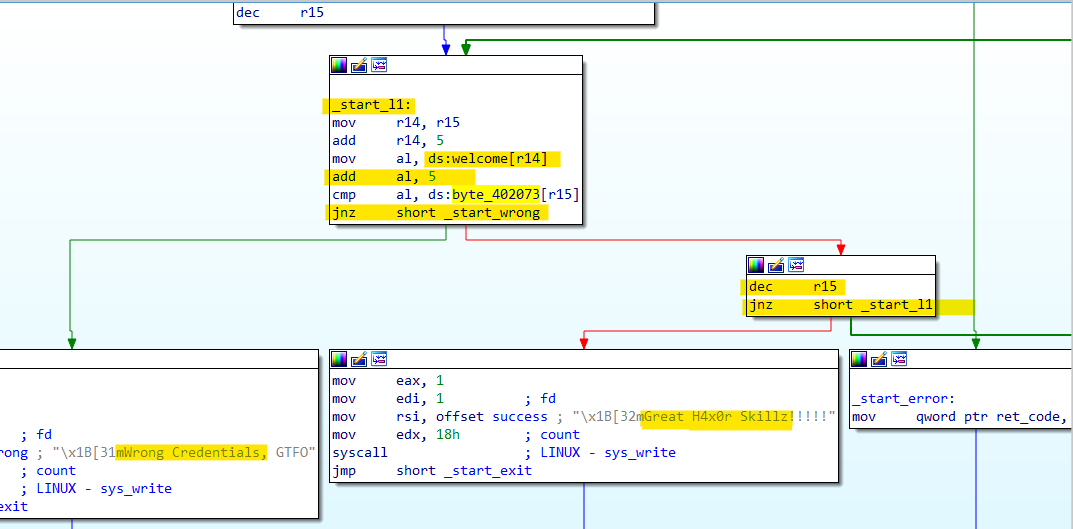


Nhập thử name quynh và pass là 123 để debug

Chương trình lưu chuỗi “Hello ” vào vùng nhớ có địa chỉ welcome 402094, sau đó lưu giá trị Name ở buf vào vùng nhớ có địa chỉ 40209A như hình :

Phân tích code kết hợp debug quan sát giá trị các thanh ghi, ta thấy ban đầu r15 chứa giá trị là độ dài của chuỗi pass, r14 = r15 +5 (bỏ qua chuỗi “Hello ”), chương trình thực hiện so sánh (giá trị tại địa chỉ byte\_402073[r15]) +5 (vùng nhớ tại địa chỉ 402074 lưu chuỗi pass) với giá trị tại địa chỉ welcome[r14], tức là so sánh kí tự cuối của pass với kí tự tiếp cách 5 trong bảng mã ASCII của kí tự cuối của Name. Sau đó giảm r15 và lặp lại quá trình trên tới khi r15=0.

Vậy suy ra độ dài pass bằng Name và pass[i]= chr (ord(Name[i])+5).



Sẽ có rất nhiều nghiệm. Chọn Name là ab và Pass là fg

Kiểm tra

