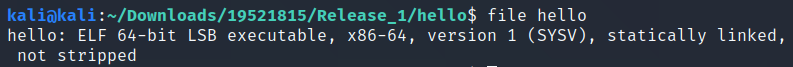
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

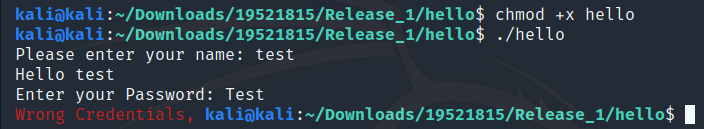
**RE CHALLENGES: HELLO**

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

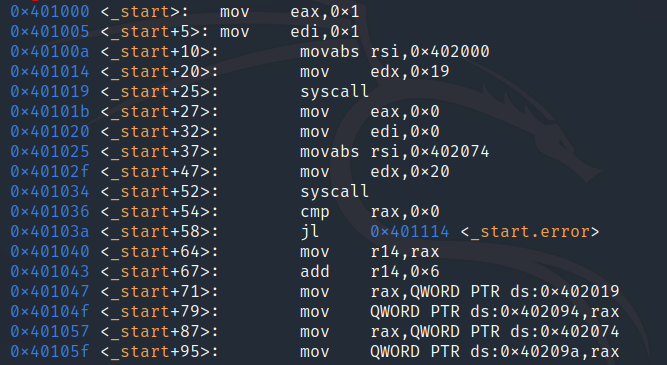
Đây là file ELF 64-bit chạy trên Linux.



Thử chạy chương trình trên terminal thì giao diện yêu cầu nhập name và password. Thử nhập như trên hình thì chương trình báo “Wrong Credentials” tức là sai. Ý tưởng bài này có thể là nhập name và password sẽ phụ thuộc vào giá trị của name.

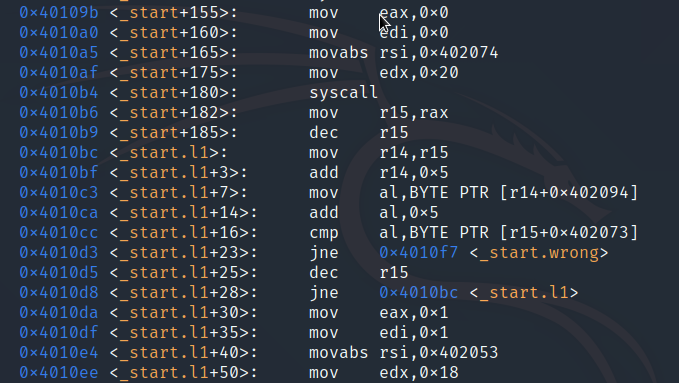


Thực hiện debug chương trình trên GDB, ta sẽ disassembly hàm <\_start> đầu tiên. Hình dưới cho chúng ta biết giá trị chúng ta nhập name được lưu ở địa chỉ 0x402074. Nếu mình không nhập thì chương trình sẽ báo lỗi bằng hàm <\_start.error>. sau đó name tiếp tục lưu vào địa chỉ 0x40209a.



Thực hiện nhập password được lưu vào địa chỉ 0x402074. Hình dưới xuất hiện một vòng lặp lần lượt kiểm tra từng kí tự của password có bằng kí tự ở vị trí tương ứng cộng 5 hay không. Ví dụ “F” = “A” + 5.

Nếu vượt qua vòng lặp này thì chương trình sẽ báo thành công, nếu không sẽ nhảy đến hàm <\_start.wrong> để báo sai.



Khi đó chúng ta chỉ cần nhập name bất kì ròi từng kí tự của password sẽ là kí tự ở vị trí tương ứng của name cộng thêm 5. Ở đây chúng ta sẽ nhập ABC thì password sẽ là FGH thì chương trình báo thành công với dòng chữ “Great H4x0r Skillz”. Vì “F” = “A” + 5, “G” = “B” + 5, “H” = “C” + 5. Có thể kết luận là chương trình có nhiều đáp án thỏa mãn.

