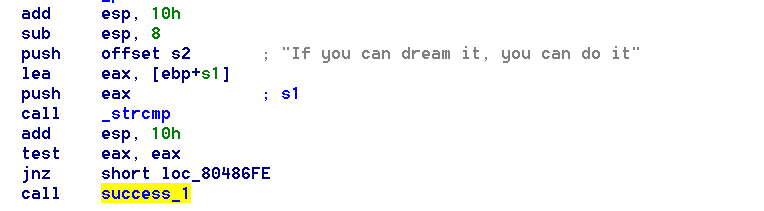
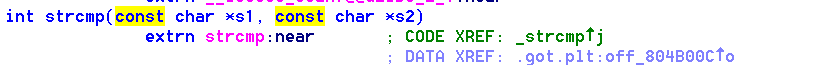
Bài 2.1:

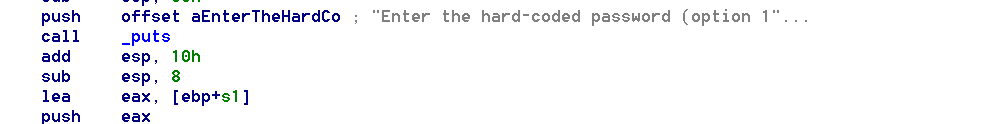


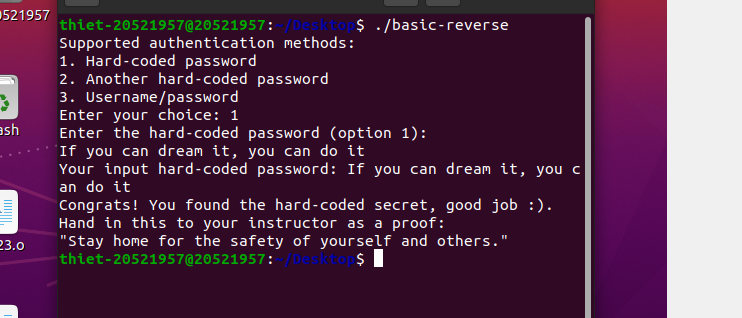
* Trước khi in hàm success ta thấy có gọi hàm \_strcmp



* Trong hàm strcmp thấy có truyền vào 2 tham số kiểu ký tự là s1 và s2



* Ở đây ta thấy tham số vị trí lưu của scanf là [ebp + s1]. Do đó, [ebp + s1] sẽ được dùng làm địa chỉ tham chiếu đến chuỗi input mà người dùng đã nhập để kiểm tra xem chuỗi được nhập có đúng yêu cầu không. 
* Trước khi gọi hàm \_strcmp ta thấy có truyền vào 2 tham số là s1 và 1 chuỗi định dạng “If you can dream it, you can do it”
* Mà trong hàm strcmp so sánh 2 chuỗi s1 và s2
* Pass: ” If you can dream it, you can do it”
* Kết quả sau khi nhập pass



Bài 2.2

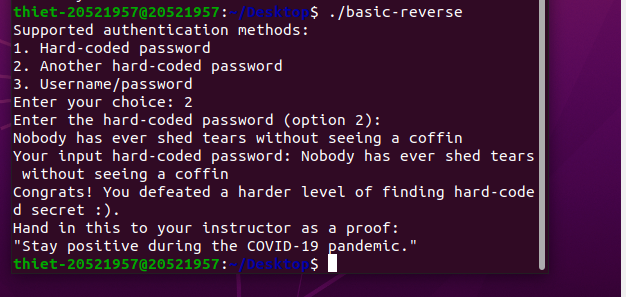
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta thấy sau khi người dùng nhập thì sẽ được lưu vào s1
* Khi xem mã giả ta thấy sẽ lấy chuỗi thứ 8 trong mảng sau đó so sánh với chuỗi s1 mà người dùng nhập



* WHAT\_THAT là 1 mảng nhiều chuỗi, mỗi phần tử của mảng này có kích thước 4 bytes và là 1 địa chỉ của 1 chuỗi nào đó
* Khi ta nhảy đến địa chỉ chuỗi thứ 8 thì ta được chuỗi “Nobody has ever shed tears without seeing a coffin”
* Pass: “Nobody has ever shed tears without seeing a coffin”
* Kết quả sau khi nhập pass

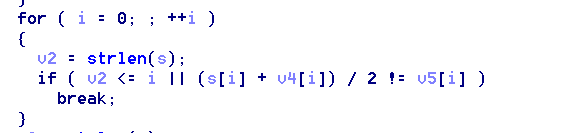


Bài 2.3

* Phân tích, tìm cặp username/password phù hợp của basicreverse với phương pháp chứng thực 3. Báo cáo nội dung thông tin bí mật tìm được.
* Sau khi sử dụng công cụ IDApro để dịch ngược và ở chế độ mã giả ta thấy được chương trình tính toán mảng v4 thông qua các giá trị trong mảng v7 đã cho trước đó

Ảnh có chứa văn bản

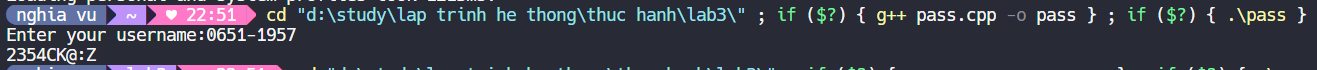
Mô tả được tạo tự động

* Sau đó là đoạn mã so sánh mật khẩu của người dùng đã nhập với giá trị v4 + username đã nhâp chia cho 2 
* Vì vậy ta viết một chương trình để tính toán được giá trị khớp chương trình đã cho sẽ truy được mật khẩu

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sử dụng kết quả của chương trình ta thu được kết quả như sau:
* Kết quả từ trương trình tính toán



* Sau khi nhập pass đã tính toán :Ảnh có chứa văn bản

  Mô tả được tạo tự động