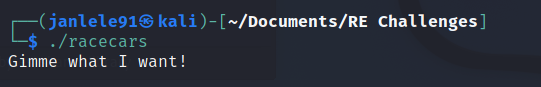
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

**RE CHALLENGES 2: RACECARS**

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

Đây là file thực thi ELF 64-bit. Thực hiện chạy thử file trên kali linux thì cho ra dòng “**Gimme what I want!**”, điều này có nghĩa là ta cần thực hiện một việc gì đó để đạt được yêu cầu của chương trình. Dự đoán ở đây có thể là truyền thêm vào tham số đầu vào hay thực hiện chỉnh sửa tên file.

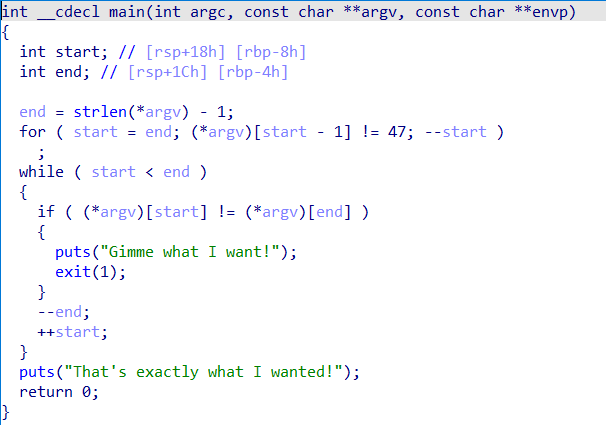


Thực hiện mở IDA Pro bản 64-bit thực hiện quá trình dịch ngược. Thực hiện xem strings có trong file thì thấy xuất hiện 2 dòng thông báo trong đó có thông báo giống như trên. “**That’s exactly what I wanted!**” chính là mục tiêu chúng ta cần hướng đến.



Thực hiện truy vết string trên thì thấy nó nằm trong hàm **main**.





Tiếp tục đọc code thì có thể dễ dàng nhận thấy chương trình đang thực hiện phân tích trên **arvg[0]** ở đây chính là **./racecars**. Ý nghĩa của đoạn code trên chỉ đơn giản là kiểm tra xem string sau dấu ‘**/**’ có phải là một **chuỗi đối xứng** hay không. “**racecars**” không phải chuỗi đối xứng nên chương trình in ra “**Gimme what I want!**”. Vì vậy chúng ta cần đổi tên file thành một tên đối xứng, ví dụ ở đây là “**racecar**”. Thực thi chương trình với tên file mới ta thấy thành công.

