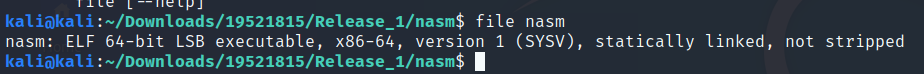
**LẬP TRÌNH HỆ THỐNG– LỚP NT209.L21.ANTN**

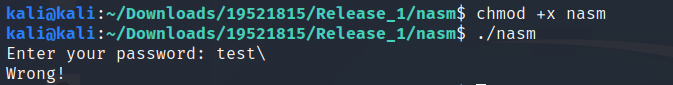
**RE CHALLENGES: NASM**

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

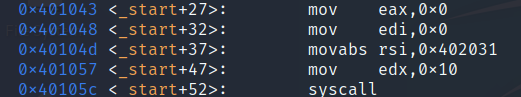
Đây là một file ELF 64-bit chạy trên linux.



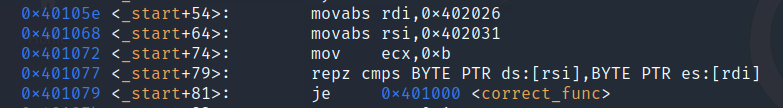
Thử chạy chương trình trên terminal thì giao diện đơn giản chỉ là nhập password nếu đúng thì báo về thành công, ngược lại sẽ báo “Wrong!”. Thử nhập “test\” thì chương trình báo không thành công. Ý tưởng chương trình có lẽ sẽ thực hiện string compare giá trị mình nhập vào và chuỗi password đúng để trả về kết quả tương ứng.



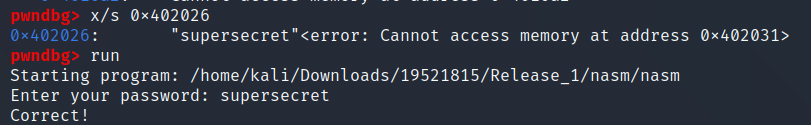
Chạy debug chương trình bằng GDB, thì xuất hiện các danh sách các hàm. Ta sẽ đi vào disassembly hàm \_start. Hình dưới là bước nhập password từ bàn phím, giá trị đó được lưu vào địa chỉ 0x402031.



Hình dưới là bước so sánh password mình vừa nhập và password gốc để cho ra kết quả. Cụ thể vì ở trên địa chỉ 0x402031 lưu password vừa nhập nên địa chỉ 0x402026 ở đây chính là lưu password gốc cần tìm. Ở đây chương trình thực hiện so sánh từng byte một của 2 biến trên. Nếu kết quả trả về là bằng nhau, chương trình sẽ je đến hàm <correct\_func>, chính là hàm thông báo kết quả thành công.



Do đó để thành công chúng ta phải nhập một chuỗi đúng bằng giá trị ở địa chỉ 0x402026. Thực hiện debug tại câu lệnh repz cmps và sử dụng câu lệnh x/s trên gdb để xem giá trị tại 0x402026 thì thấy đó là chuỗi “supersecret”. Đây chính là password cần tìm.



Chạy lại chương trình nhập với password là “supersecret” thì chương trình báo “Correct!”.