CrackMe 2

Run cho đến khi hiện thị như hình

A screenshot of a computer

Description automatically generated

Ở dưới ta thấy nó đang đọc file keyfile.txt và hàm CreateFileA. Đọc định nghĩa hàm, hàm trả về false nếu bị lỗi khi mở file.

Dòng 00401049 có lệnh move từ eax (là giá trị của CreateFileA) vào esi. Dòng 0040104B cố gắng so sánh esi với FFFFFFFF (-1), là xác định xem liệu mở file có lỗi hay không (điều này thể hiện qua dòng 0040105F (lệnh ReadFileEx).

Như vậy, ta có thể giải quyết bằng cách tạo file keyfile.txt và cho tên bất kì, sau đó mở lại file để check

A computer screen shot of a computer

Description automatically generated