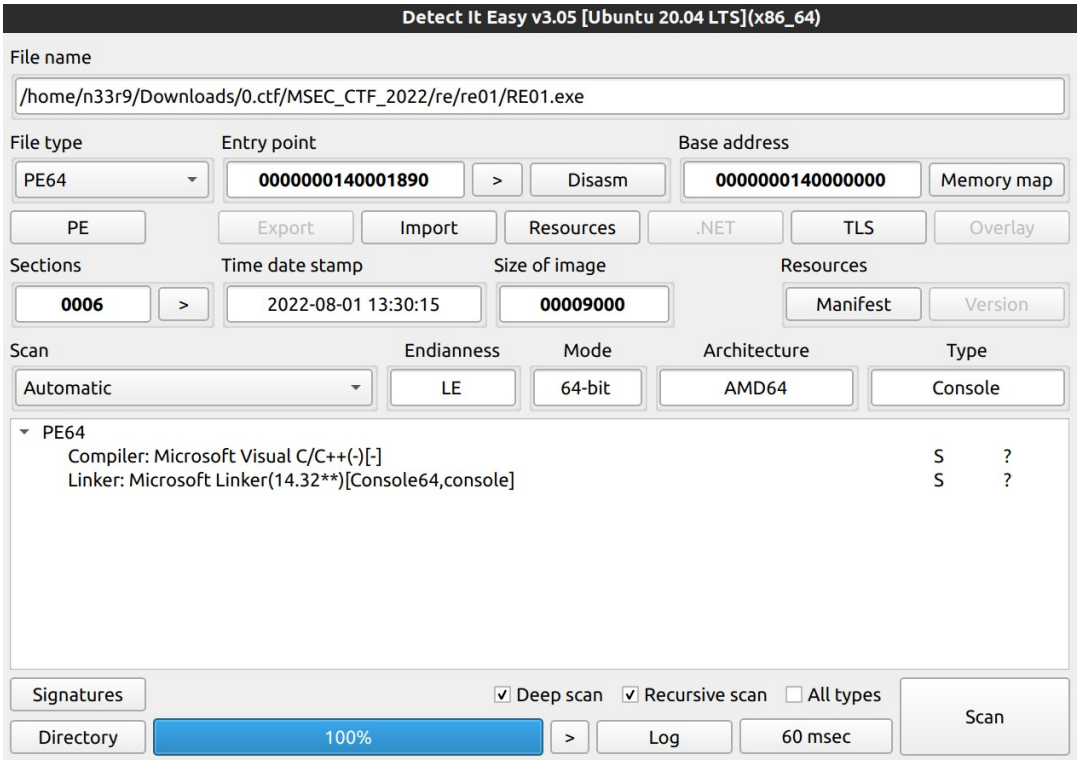
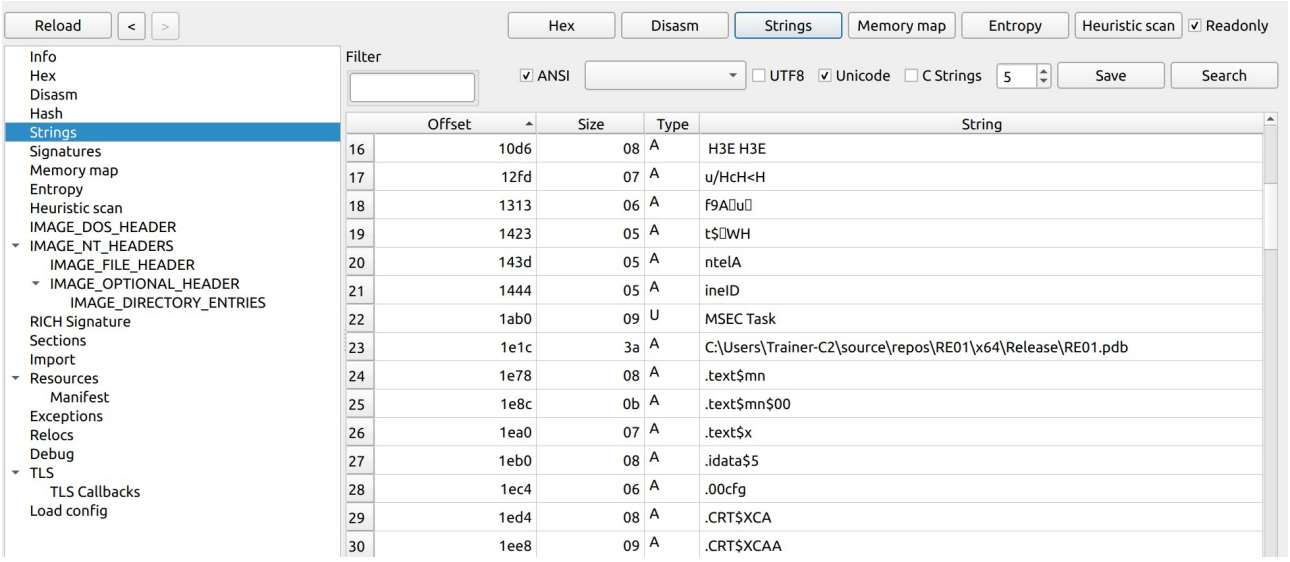
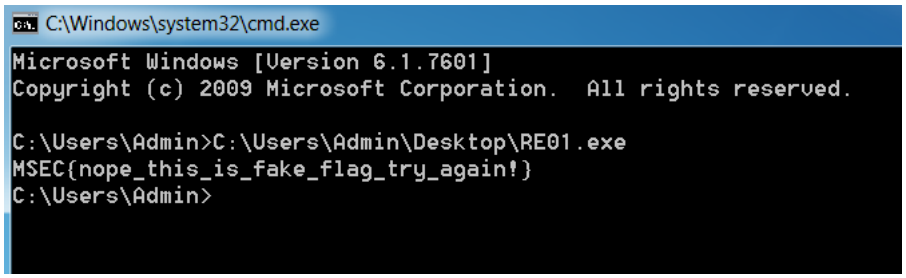
Write-up RE01

Đề bài cho ta một file exe, load file vào DIE để kiểm tra sơ bộ:

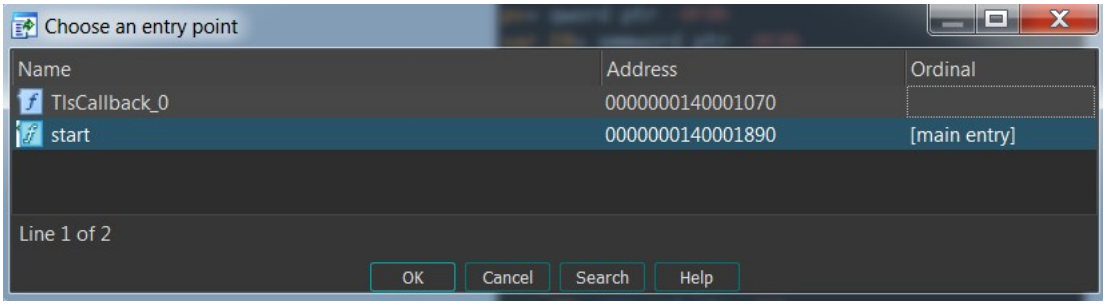




Sau khi chạy file, chương trình cho ta một flag fake:



Load file vào IDA64, ta chú ý đến hàm tlscallback_0. TLScallback sẽ được gọi và thực thi trước khi nhảy đến entry point của chương trình(main). IDA pro có thể phát hiện ra hoạt động của hàm này. Ctrl+E để kiểm tra entry point của file thực thi trong IDA, ta sẽ thấy hàm Tlscallback_0.

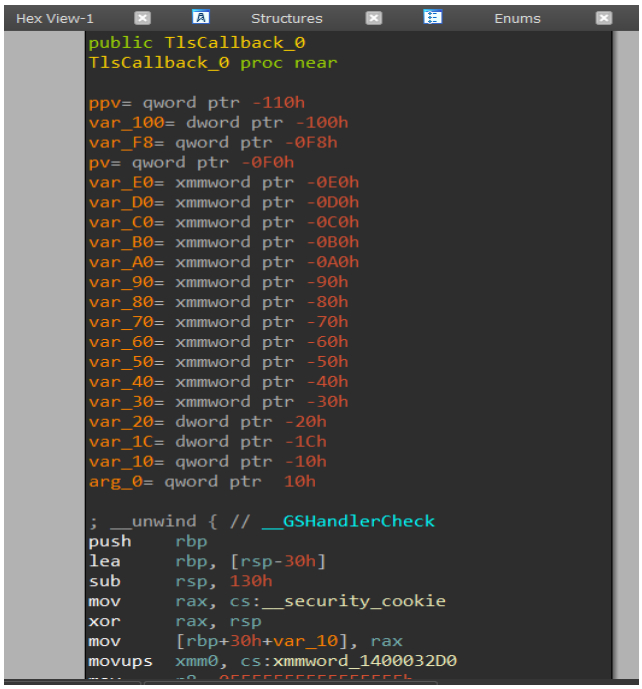


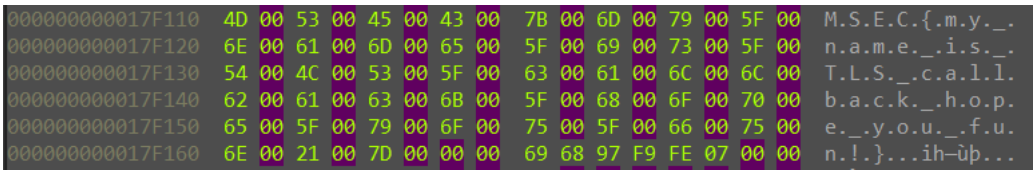
Để debug được, ta có thể config debugger in IDA chọn suspend when process created, hoặc đặt breakpoint tại hàm Tlscallback_0.

Disassemble hàm này, ta thấy cách thức hoạt động của nó và hàm main khá giống nhau, đều thực hiện biến đổi một mảng các ký tự.

Có thể flag thật được tạo ra ở hàm tlscallback, nhưng sau khi thực hiện hàm main, flag giả lại được in ra cho người dùng thấy

Sau khi thực thi xong hàm tlscallback, view memory, ta sẽ thấy flag thật được tạo ra.





Flag: MSEC{my_name_is_TLS_callback_hope_you_fun!}