Đây là một ứng dụng có giao diện sử dụng winapi. Chương trình sẽ bắt đầu từ hàm WinMain.

Graphical user interface, text, application, email

Description automatically generated

Đoạn đầu của WinMain thực hiện check quyền admin, do vậy ta phải chạy IDA bằng quyền admin để có thể debug được.

WinMain không có gì đặc biệt, chỉ cho biết function nào được sử dụng làm Procedure

Có hàm TLSCallback\_0, hàm này sẽ được gọi trước khi chương trình bắt đầu hàm main, malicious program có thể sử dụng để kiểm tra debugger hoặc làm gì đó trước khi breakpoint ở trong.

Graphical user interface, application

Description automatically generated

Hàm này có gọi NtQueryInformationProcess (debug tới đây để biết hàm nào đã được gọi) để check debugger. Nếu phát hiện debuger thì sẽ thay đổi byte thứ 10 của vùng nhớ 0x335018 thành 74h (vùng nhớ này đóng vai trò quan trọng trong việc giải lấy flag). Bypass bằng cách patch jump qua.

Graphical user interface, text, application

Description automatically generated

Quay lại Procedure của chương trình, khi bấm login thì chương trình sẽ get text đã nhập ở editbox, sau đó gọi sub\_401B40 với tham số là string đã nhập ở editbox:

Text

Description automatically generated

Đầu tiên input check phải lớn hơn 38 kí tự. Hàm sub\_331FD0 nhận vào v23 và 1 byte tại một vùng nhớ khác. Vùng nhớ này chính là vùng nhớ mà TLS\_Callback đã sửa lúc trước. Như vậy nếu TLSCallback phát hiện ra debugger thì sẽ hoạt động khác sẽ suffle một vùng nhớ đã định sẵn và ghi vào v23.