HỌC VIỆN KỸ THUẬT MẬT MÃ
**KHOA AN TOÀN THÔNG TIN**

# MODULE THỰC HÀNH
# MÃ ĐỘC

## BÀI THỰC HÀNH SỐ 05

Sử dụng ollydbg phân tích mã độc

Người thực hiện bài thực hành:

TS. Đặng Xuân Bảo

Hà Nội, 2020

# MỤC LỤC

# THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

**Tên bài thực hành**: Sử dụng ollydbg phân tích mã độc

**Học phần**: Mã độc

**Số lượng sinh viên cùng thực hiện**:

Địa điểm thực hành: Phòng máy

**Yêu cầu**:

- Yêu cầu phần cứng:
  + Máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 4GB, HDD 500GB
- Yêu cầu phần mềm trên máy:
  + Hệ điều hành Windows 10
  + VMware Worstation 15.0
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có

# CHUẨN BỊ BÀI THỰC HÀNH

**Đối với giảng viên**

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

**Đối với sinh viên**

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

# Sử dụng ollydbg phân tích mã độc

## 1.1. Mô tả

Bài thực hành hướng dẫn sinh viên sử dụng một số công cụ trong việc phân tích động một số mẫu mã độc đơn giản..

## 1.2. Chuẩn bị

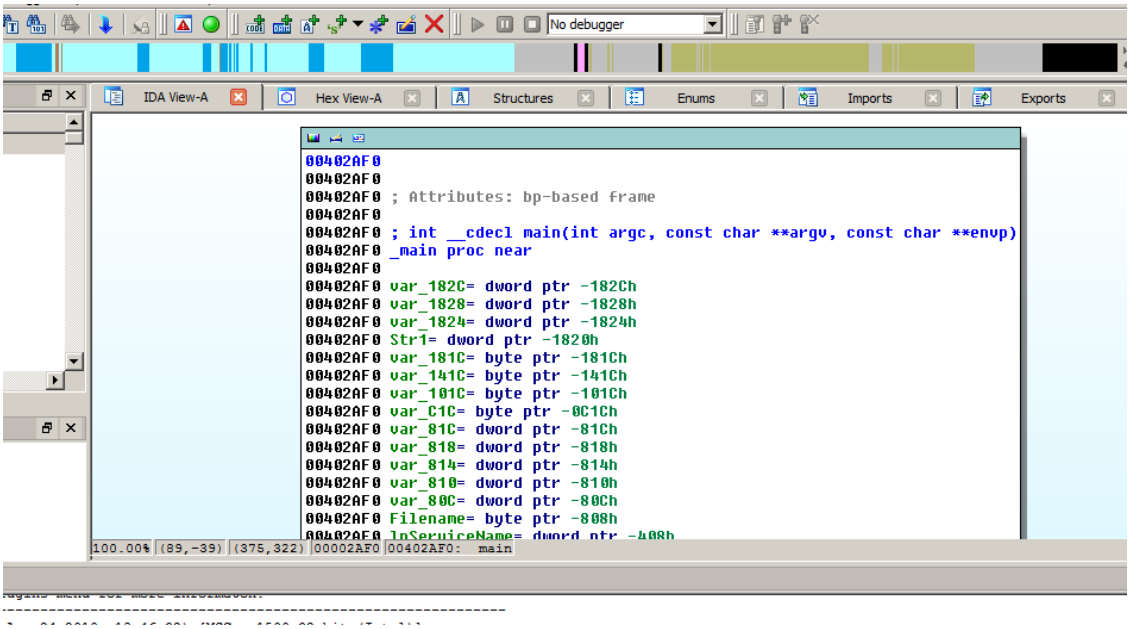
- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

## 1.3. Phân tích Lab09-01

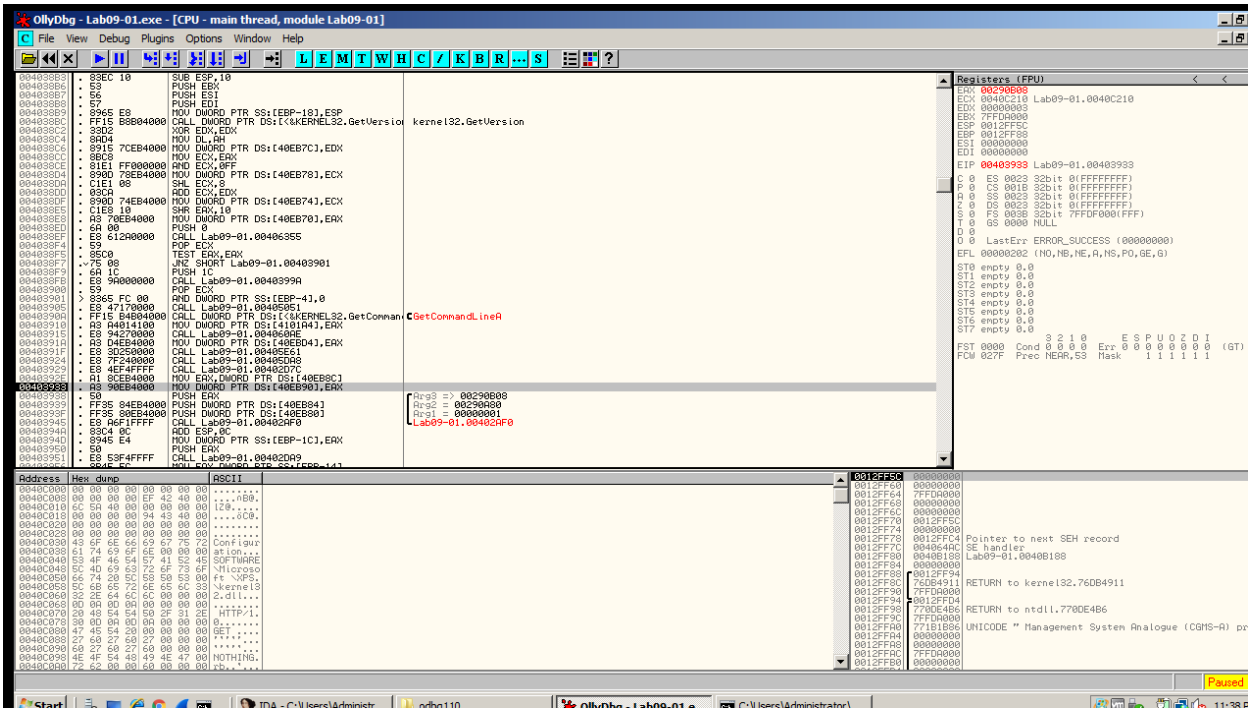
Thực hiện các yêu cầu với Lab09-01.exe có trong tài liệu Practical Malware Analysis.

**Tìm điểm bắt đầu của hàm main**

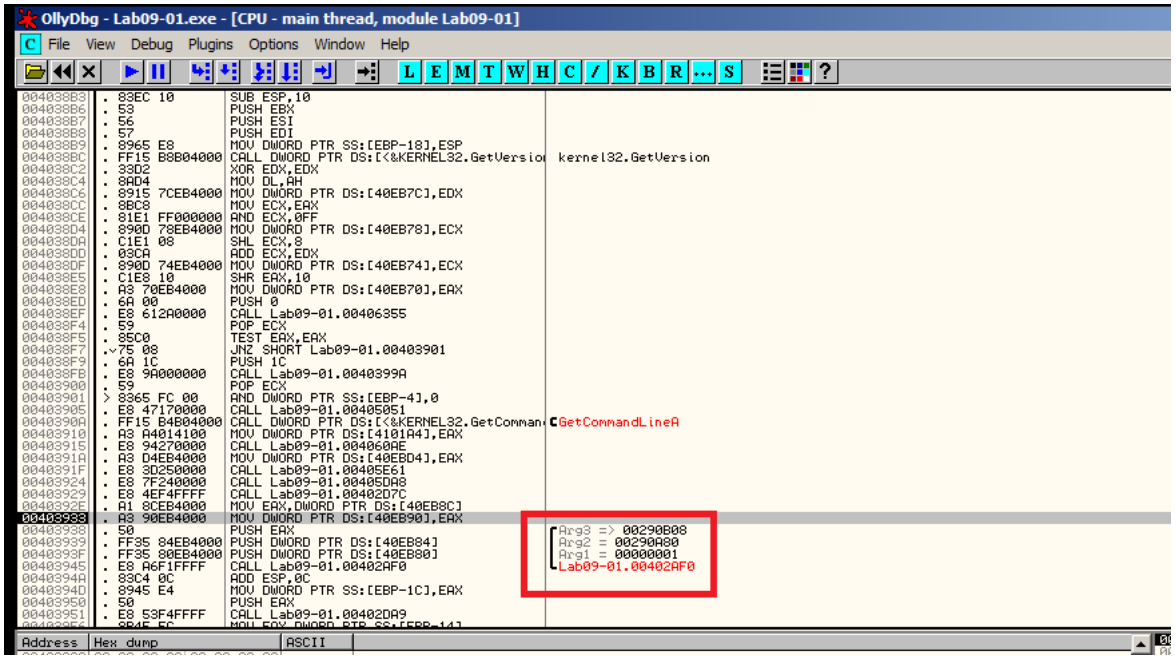
- Sử dụng IDA pro để phân tích Lab09-01.exe.
- Chọn Option → General, đánh dấu Line Prefixes, chọn OK.
- Sau đó chọn Window, " Reset Desktop"
- IDA pro sẽ hiển thị địa chỉ hàm main tại 0x402AF0



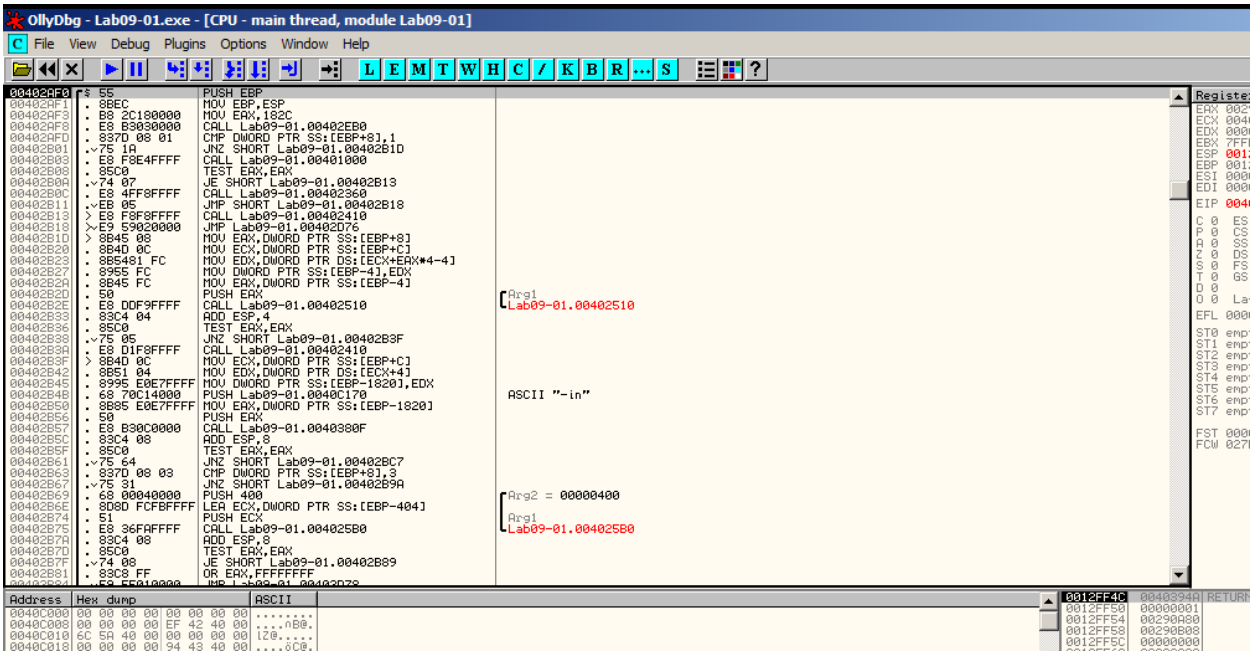

Dùng ollydbg đọc Lab09-01.exe



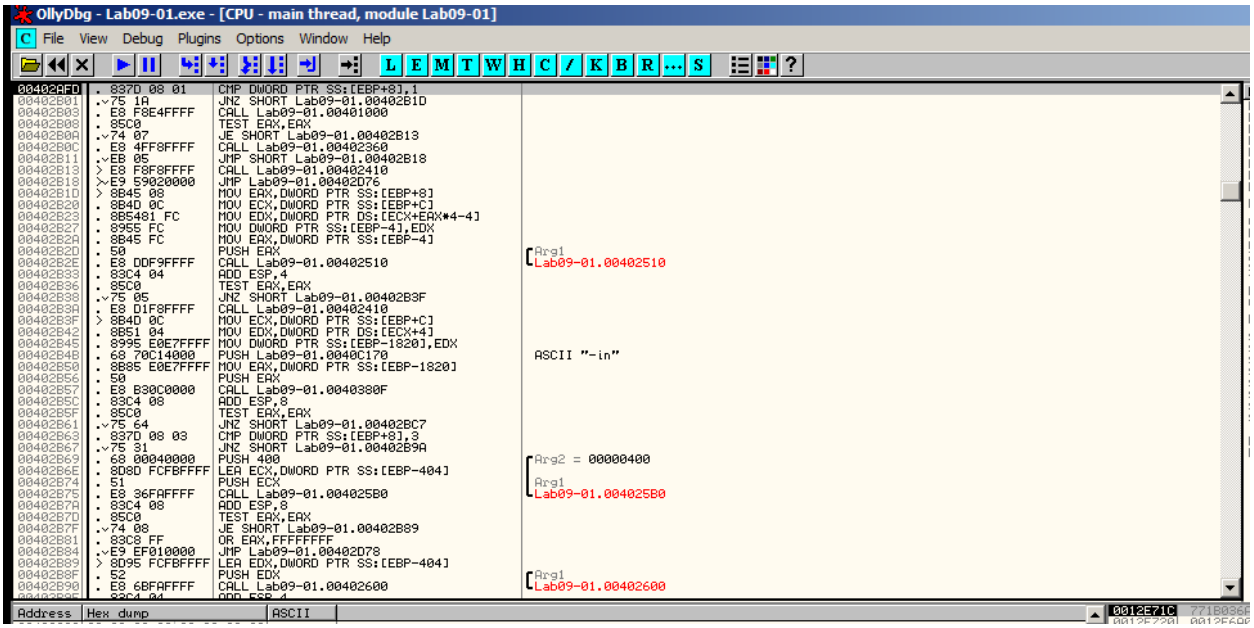
- Nhấn F8 40 lần, để đến được địa chỉ 0x403933, cuộn xuống vài dòng ta sẽ thấy được mã đối số và hàm gọi chính.



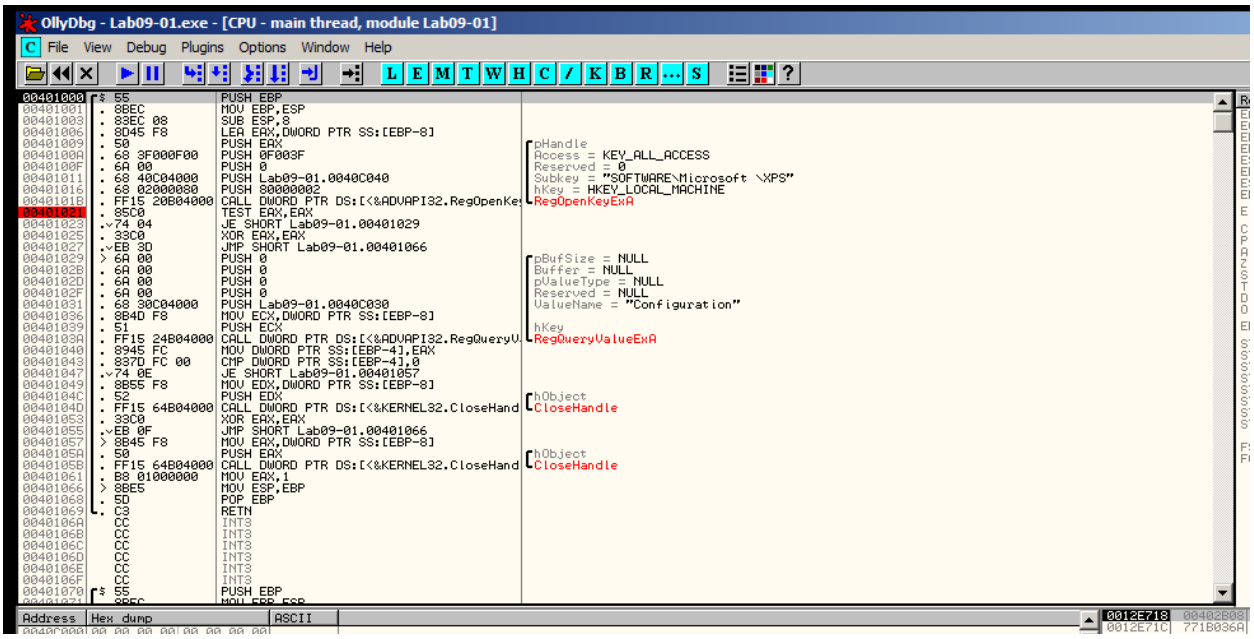
- Tiếp tục nhấn F7 5 lần để tải các tham số và gọi hàm main từ địa chỉ 0x403945, phần mã mới hiển thị bắt đầu từ địa chỉ 0x402AF0.



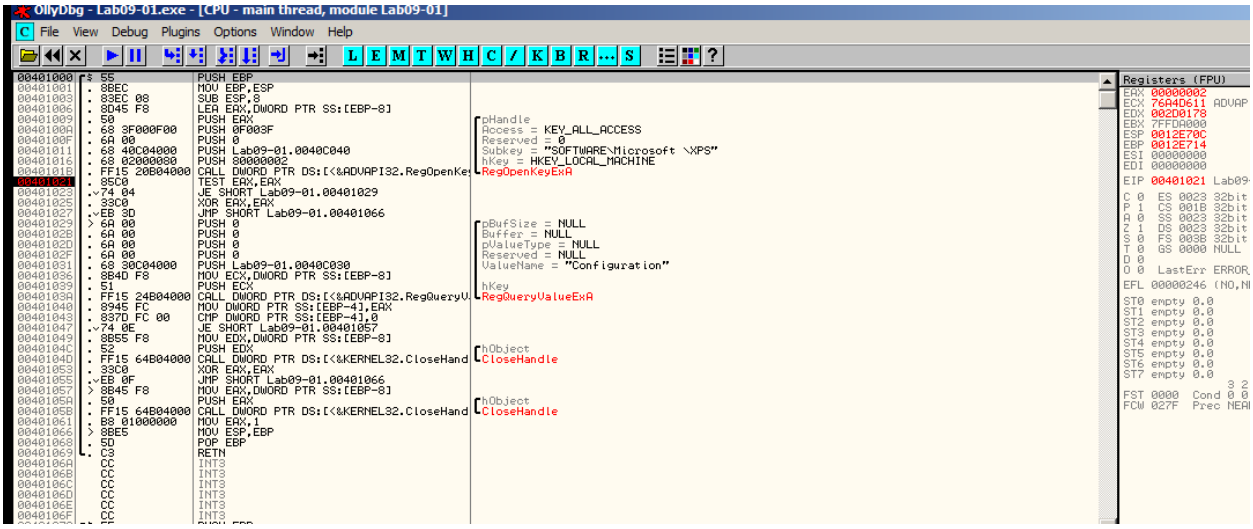

- Tiếp tục nhấn F7 21 lần, để gọi một chương trình con ngắn và đến địa chỉ 0x402AFD.



- Nhấn F7 3 lần để vượt qua bài kiểm tra, và nhảy đến địa chỉ 0x401000.
- Bây giờ chúng ta đang ở địa chỉ 0x401000
- Chương trình gọi RegOpenkeyExA tại đia chỉ 0x40101B
- Nhấp chuột trái vào dòng bắt đầu với địa chỉ 0x401021, và nhấn F2 để đặt điểm dừng tại đó. Địa chỉ đó sẽ chuyển sang màu đỏ.
- Nhấn chuột trái vào dòng bắt đầu tại địa chỉ 0x401000. Nhấn F9 để chạy điểm dừng. Kết quả ở hình bên dưới.

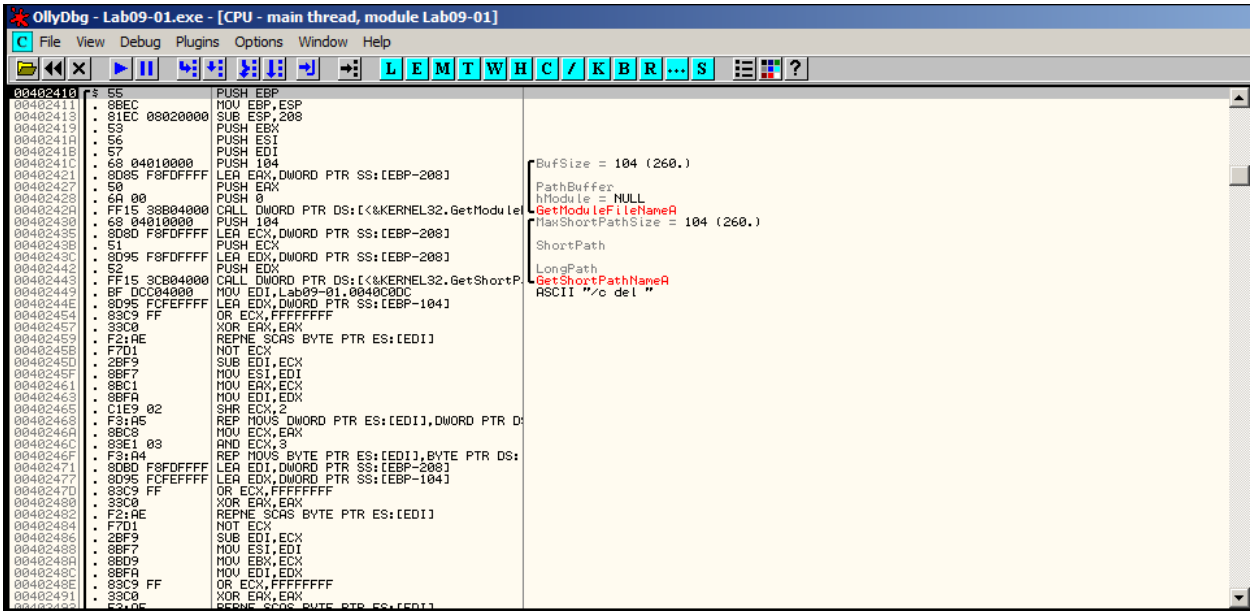



- Nhìn phía trên bên phải để xem thanh ghi EAX chứa 2.

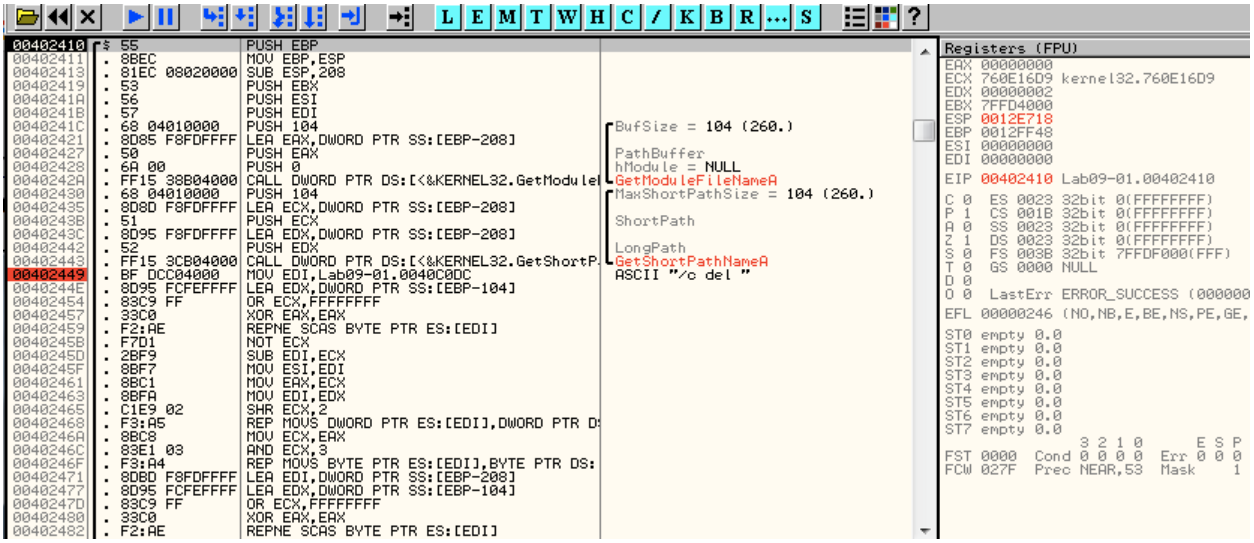



→ Đây là mã lỗi khác không.

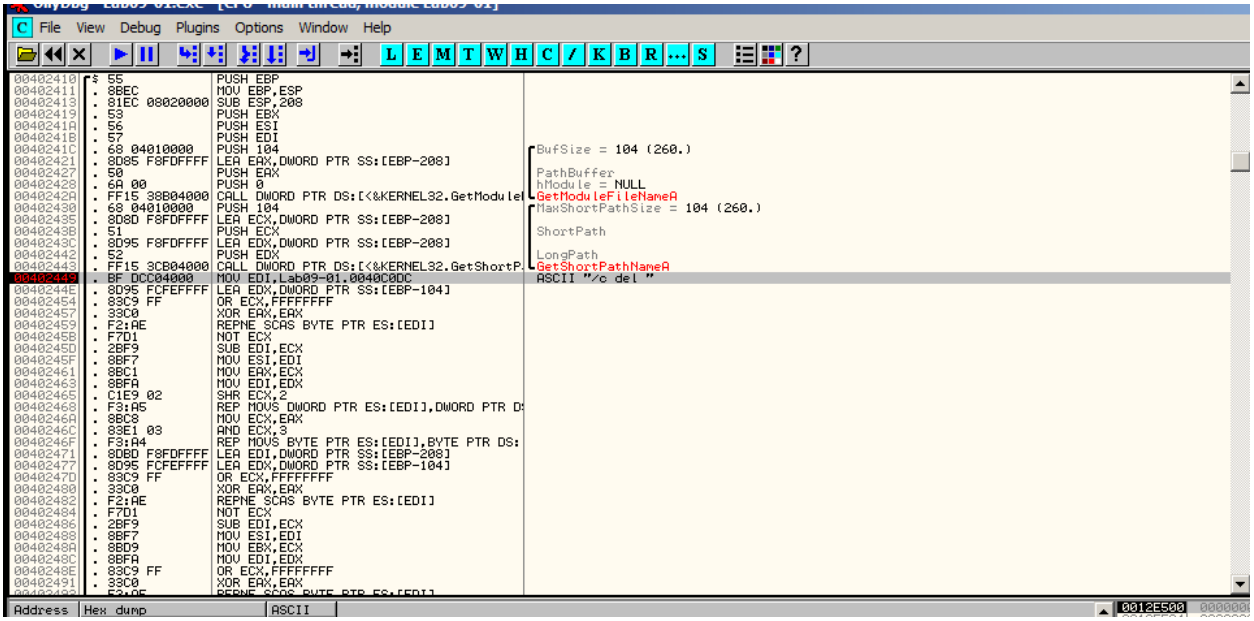
- Điều này có nghĩa là thử nghiệm thất bại, không tìm được khóa đăng ký mà nó đang tìm kiếm.
- Nhấn F7 3 lần để đến địa 0x401027
- Nhấn F7 để thực thi JMP
- Nhấn F7 3 lần để đi qua chương trình con để đến địa chỉ 0x402B08
- Nhấn F7 3 lần để đến địa chỉ 0x402410



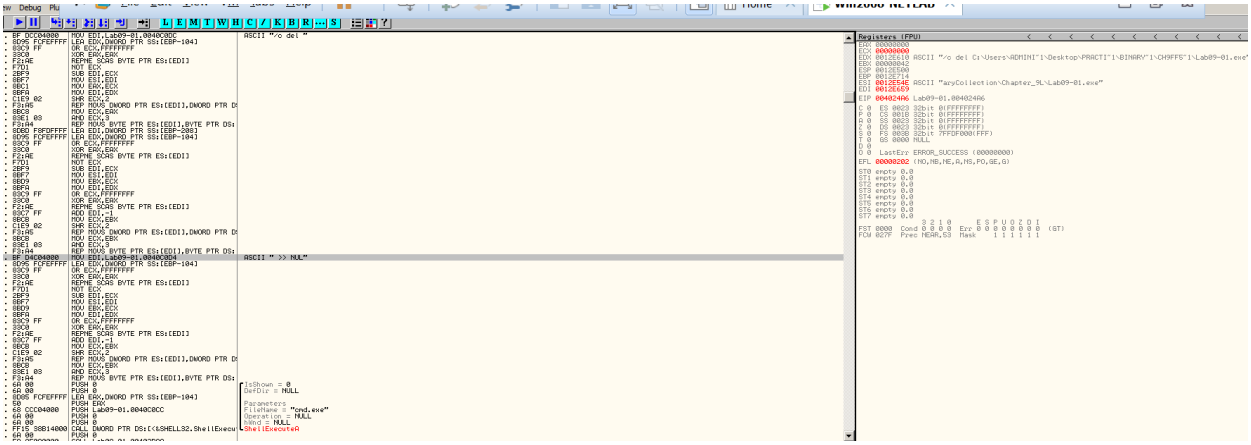
- Hàm này sử dụng GetModuleFileName để có được đường dẫn đến tệp thực thi hiện tại và xây dựng chuỗi ASCII
- Để nhìn thấy điều đó, hãy đặt một điểm dừng ngay sau GetShortPathName, để địa chỉ của nó chuyển sang màu đỏ.




- Nhấp vào dòng bắt đầu 0x402410 để tô sáng nó
- Nhấn F9 để chạy điểm dừng.
- Bây giờ bạn sẽ dòng có kết thúc bằng “ASCII “/c del””



- Bằng cách giữ F7 hoặc nhấn vào nó nhiều lần.
- Xem mã từ từ đi qua như một đường dẫn dài trong EDI. Sau đó tên đường dẫn lật nhanh qua một số thanh ghi, kết thúc bằng EDX.
- Dừng lại khi bạn nhìn thấy một chuỗi tron EDX, bắt đầu với ASCII "/c del C:\"



Chú ý:

Nếu nhấn F7 quá nhiều lần, thì EDX sẽ trống, để trở về điểm này bạn cần thực hiện các bước sau:

- Trên menu OllyDbg, chọn Debug, Restart
- Chọn Yes
- Nhấn F9 để chạy điểm dừng 0x401021
- Nhấn F9 để chạy điểm dừng 0x402449
- Giữ hoặc nhấn F7 để đến điểm mong muốn.