

ASpack

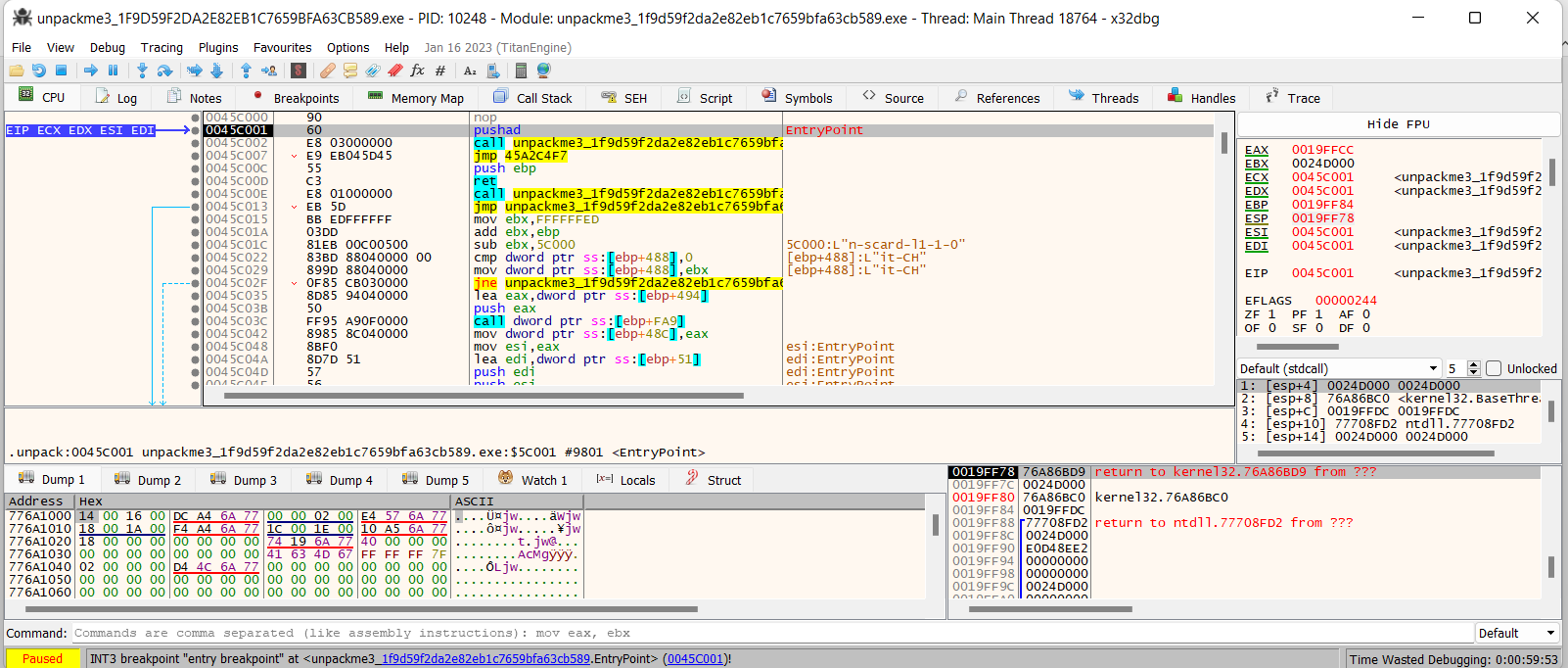
1. File sẽ thực thi phần tại phần code đã được thêm vào
2. Lưu lại trạng thái của các thanh ghi hiện tại bằng pushad
3. Giải nén phần code thực thi ban đầu

* Dựa vào thuật toán nén để khôi phục ngoài các câu lệnh cơ bản còn sử dụng các API
* GetModuleHandleA
* GetProcAddress
* Từ 2 hàm trên lấy được 3 con trỏ hàm của
  + - * + VirtualAlloc : cấp phát bộ nhớ ảo
        + VirtualFree : giải phóng
        + SVirtualProtect : thay đổi quyền truy cập ( hàm này sử dụng sau để đảm bảo code sau khi khôi phục sẽ được bảo vệ)

1. Khôi phục lại IAT

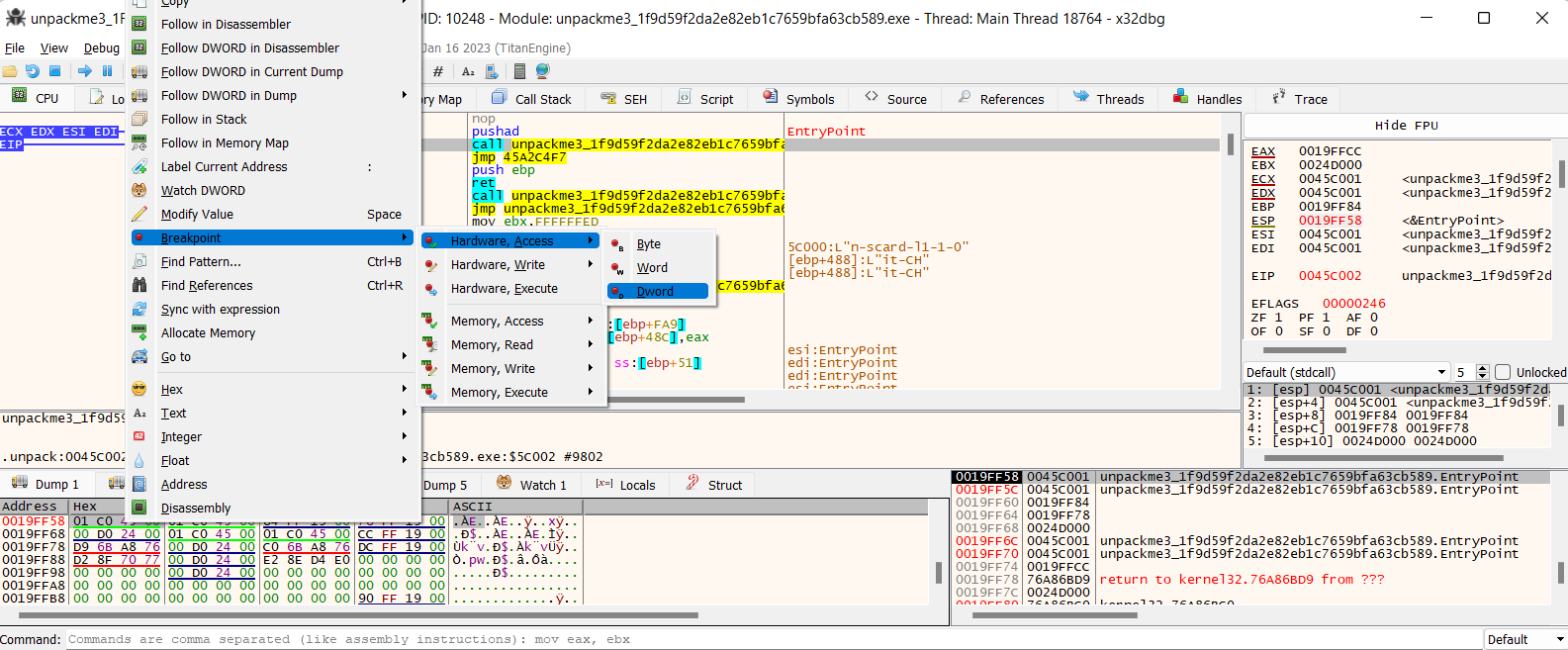
* GetModuleHandleA
* GetProcAddress

1. Khôi phục lại trạng thái thanh ghi bằng popad
2. Jump tới OEP gốc của file thực thi ban đầu

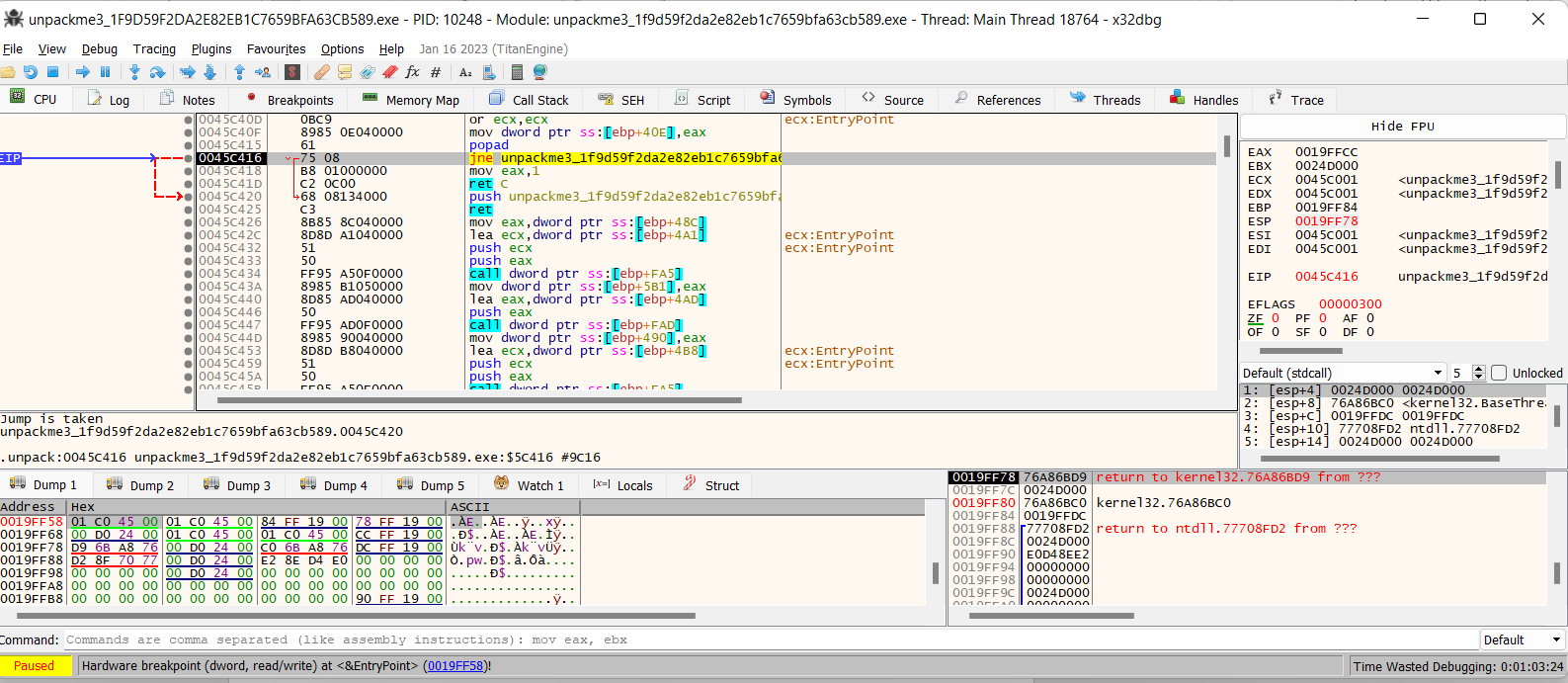


Load file vào IDA . F9 ta tới được câu lệnh push ad đây là dấu hiệu để tìm OEP.

Set breakpoint on access



F9 thêm 1 lẫn nữa



Tiếp tục đi theo chương trình ta tìm được OEP

