6

Lab

Simple Rootkit

Thực hành Cơ chế hoạt động của Mã độc

Lưu hành nội bộ 2024

A. TỔNG QUAN

- Tìm hiểu cơ chế hoạt động của Rookit trên môi trường Windows
- Tích hợp Rootkit vào driver trên môi trường Windows

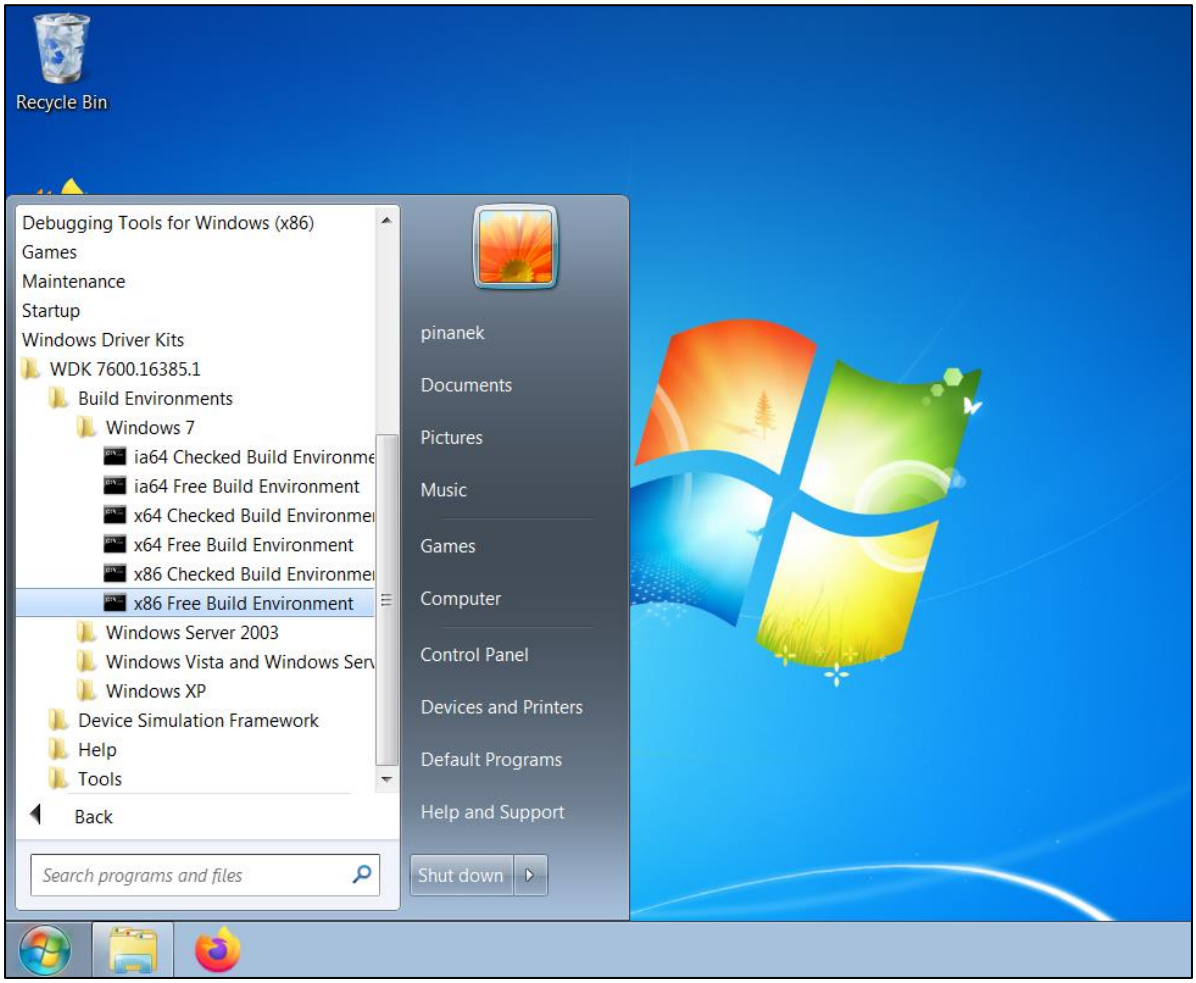
B. CHUẨN BỊ MÔI TRƯỜNG

- Máy ảo Windows 7 32 bit (ISO).
- Security update for Windows 7 (KB3033929).
- Cài đặt lên máy các chương trình sau:
  - Window Driver Rootkit 7.1 (tải tại đây)
    Window Driver Rootkit (WDK) là công cụ để biên dịch code (C, C++) thành driver chạy được trên môi trường Windows, WDK hỗ trợ nhiều môi trường Windows khác nhau như: WinXP, Win7, Win2k3.... Chú ý cần cài Visual Studio trước khi cài WDK.
  - Sysinternals-Suite (tải tại đây)
    Sysinternals-Suite là bộ công cụ hỗ trợ chúng ta theo dõi quá trình làm việc của driver (Trong bài thực hành này chúng ta sẽ sử dụng chương trình **Dbgview**).
  - OSR Driver Loader (tải tại đây)
    OSR Driver Loader là chương trình điều khiển (register, start, stop, remove) driver trên Windows, rất hữu ích trong quá trình phát triển, thử nghiệm driver.

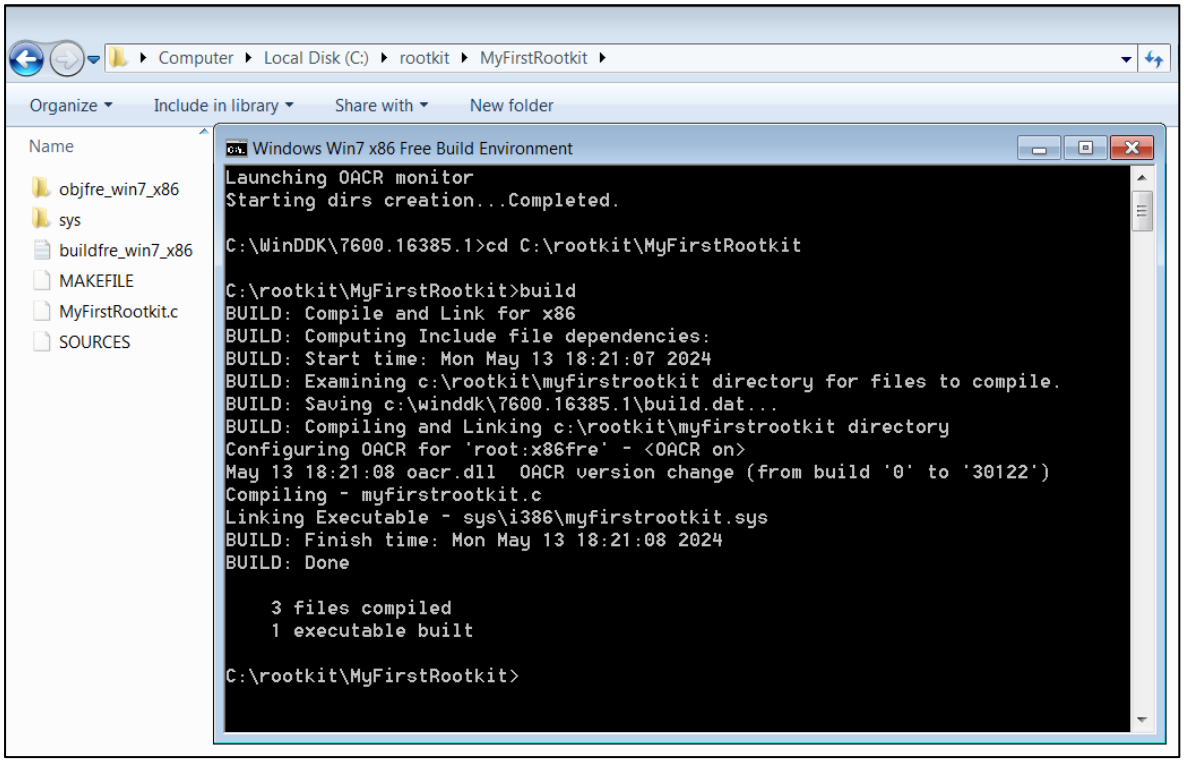
C. THỰC HÀNH

C.1 Tạo lập môi trường phát triển Windows driver

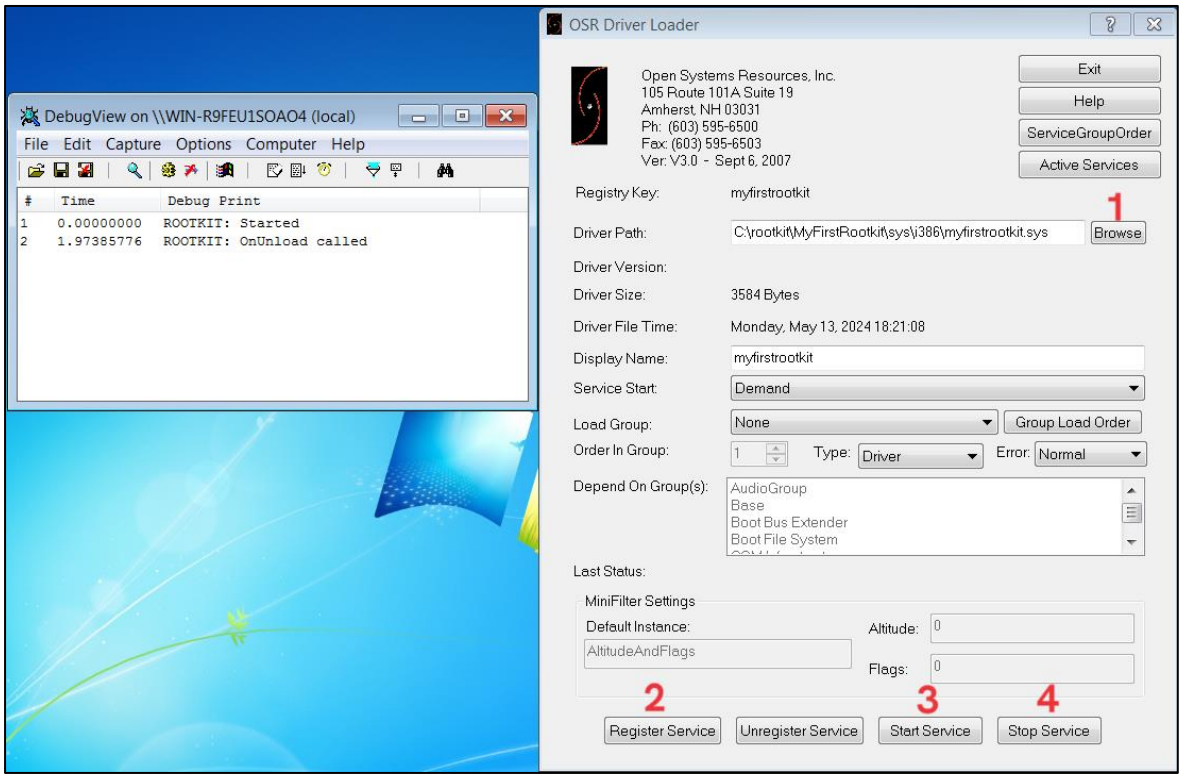
1. Tạo Driver Rootkit đầu tiên bằng cách copy thư mục MyFirstRootkit trong thư mục mã nguồn theo đường dẫn *C:\rootkit\MyFirstRootkit* sau đó dùng Windows Driver Rootkit (Windows 7 Free) để biên dịch thử.



2. Command line mở lên, di chuyển thư mục vào *C:\rootkit\MyFirstRootkit*, sau đó chạy lệnh build nếu màn hình xuất hiện như sau là thành công. Lúc này trong thư mục C:\rootkit\MyFirstRootkit có thêm thư mục sys, đây là thư mục chứa driver của ta.



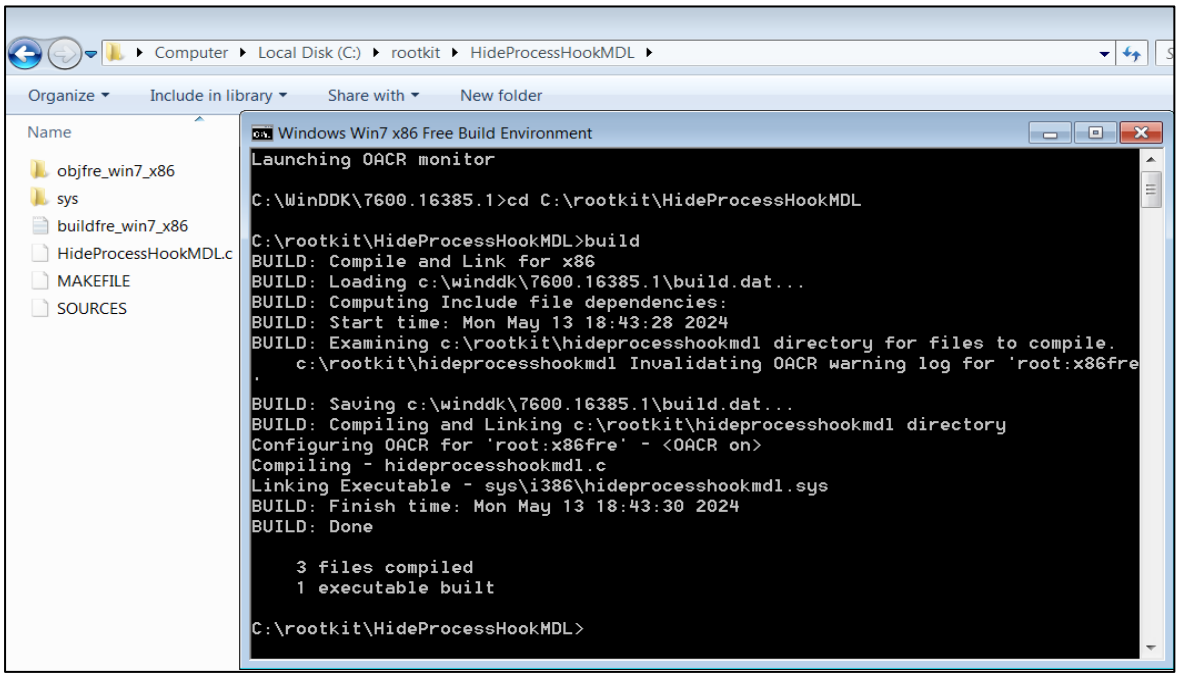
3. Dùng OSR Driver Loader để chạy đăng ký và chạy driver vừa tạo, dùng Debug View để theo dõi. Ở bước này chúng ta đã tạo và chạy được một driver rootkit đơn giản đầu tiên khi chạy lên (ROOTKIT: started) và khi dừng (OnUnload Called).



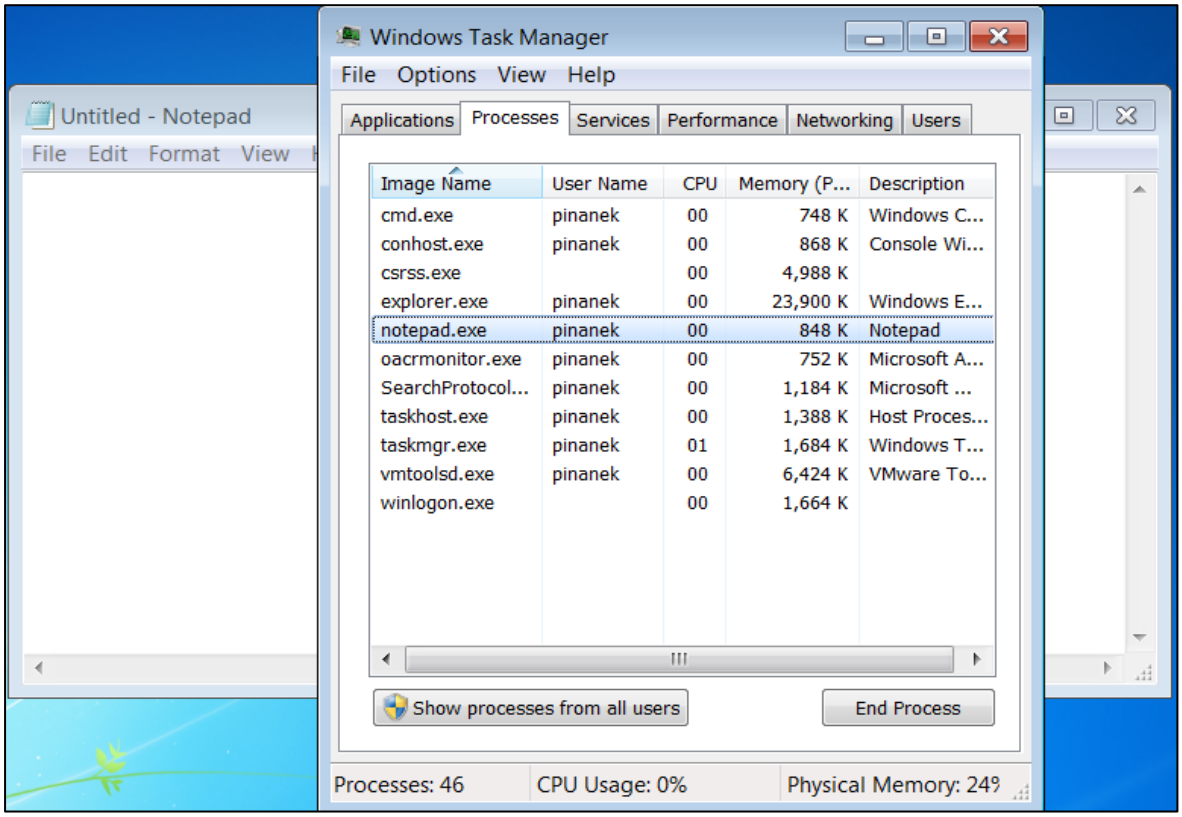
C.2 Tạo Rootkit ẩn một chương trình trong Task Manager

Ở phần này sẽ viết thêm code để thực hiển ẩn chương trình notepad.

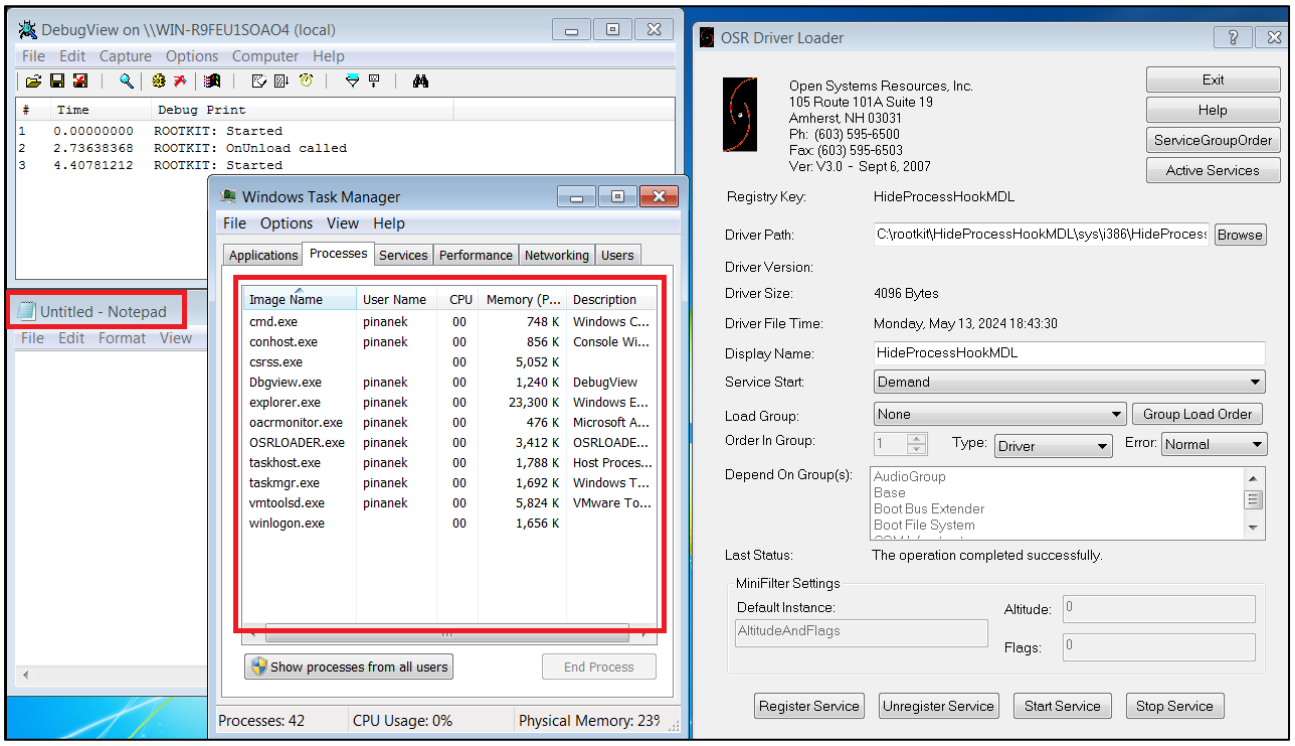
1. Copy HideProcessHookMDL từ source code *vào C:\rootkit\ HideProcessHookMDL*. sẽ có 3 tập tin cần quan tâm đó là:
   - **HideProcessHookMDL.c** viết bằng ngôn ngữ C để chạy driver của chúng ta
   - **SOURCE**: tập tin cấu hình giúp Windows Driver Kit biên dịch **HideProcessHookMDL.c thành HideProcessHookMDL.sys**
   - **MAKEFILE**: tập tin mặc định của WDK
2. Dùng Windows Driver Kit để biên dịch thành driver.



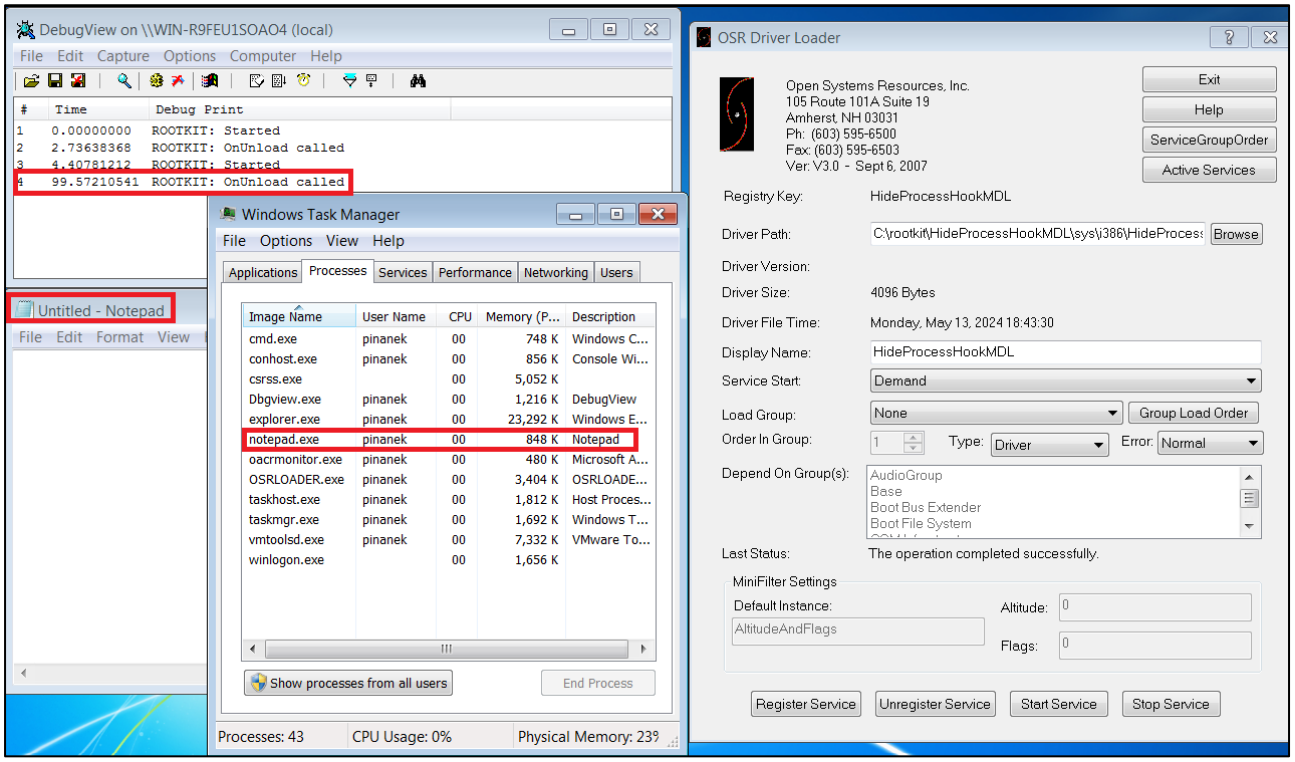
3. Chạy *Notepad* và *Task Manager* lên để kiểm tra chương trình notepad vẫn còn hiển thị được.



4. Đăng ký (Register Service) và chạy (Start Service) driver lên bằng ORS Driver Loader và quan sát bằng DebugView.
   Lúc này driver mình được biên dịch:
   C:\rootkit\HideProcessHookMDL\sys\i386\HideProcessHookMDL.sys
5. Quan sát Task Manager. Lúc này *notepad* đã được ẩn đi, trong khi chương trình notepad vẫn hoạt động bình thường.



6. Dừng (Stop Service) driver lại và kiểm tra notepad có trong Task Manager không?



C.3 Tạo Rootkit ẩn một chương trình tùy ý

> **Yêu cầu 1** **Tìm hiểu code và thay đổi code sao cho khi chạy driver lên sẽ ẩn một chương trình tùy ý, hiển thị thông tin sinh viên khi driver được chạy.**

D. YÊU CẦU

Sinh viên quay video lại quá trình làm việc và nộp link youtube* (chế độ unlisted) *lên courses.

- Sinh viên tìm hiểu và thực hành theo hướng dẫn theo cá nhân.
- Báo cáo kết quả chi tiết những việc (**Report**) đã thực hiện, quan sát thấy, giải thích cho quan sát .

Báo cáo:

- Làm báo cáo trên file **mẫu**.
- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Trong file báo cáo yêu cầu **ghi rõ** nhóm sinh viên thực hiện.
- Đặt tên theo định dạng: [Mã lớp]-Lab1_MSSV1-MSSV2.pdf
  Ví dụ: [NT330.O2X.ATXX.X]-Lab2_2452xxxx-2452yyyy.pdf
- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trễ,… sẽ được xử lý tùy mức độ vi phạm.

-HẾT-