**Trường Đại học Công nghệ Thông tin (UIT)**

# 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](mailto:21522620@gm.uit.edu.vn) |
| **2** | Chu Nguyễn Hoàng Phương | 21522483 | [21522483@gm.uit.edu.vn](mailto:21522483@gm.uit.edu.vn) |

**1. NỘI DUNG THỰC HIỆN:**[**1**](#_bookmark0)

|  |  |  |  |
| --- | --- | --- | --- |
| **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

**2**

# 

# 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.

A screen shot of a computer program

Description automatically generated

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.

A computer screen shot of a computer code

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

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

A computer screen with white text

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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