BÁO CÁO THỰC HÀNH

**Môn học: Cơ chế hoạt động của Mã độc**

**Lab 6: Simple Rootkit**

*GVHD: Nguyễn Hữu Quyền*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT230.O22.ATCL.1- Nhóm 3

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Ngọc Trà My | 21520353 | [21520353@gm.uit.edu.vn](mailto:21520353@gm.uit.edu.vn) |
| 2 | Bùi Hoàng Trúc Anh | 21521817 | [21521817@gm.uit.edu.vn](mailto:21521817@gm.uit.edu.vn) |
| 3 | Lê Hoàng Oanh | 21521253 | [21521253@gm.uit.edu.vn](mailto:21521253@gm.uit.edu.vn) |
| 4 | Bùi Nguyên Phúc | 21522469 | 21522469@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | **Yêu cầu 1** | 100% |

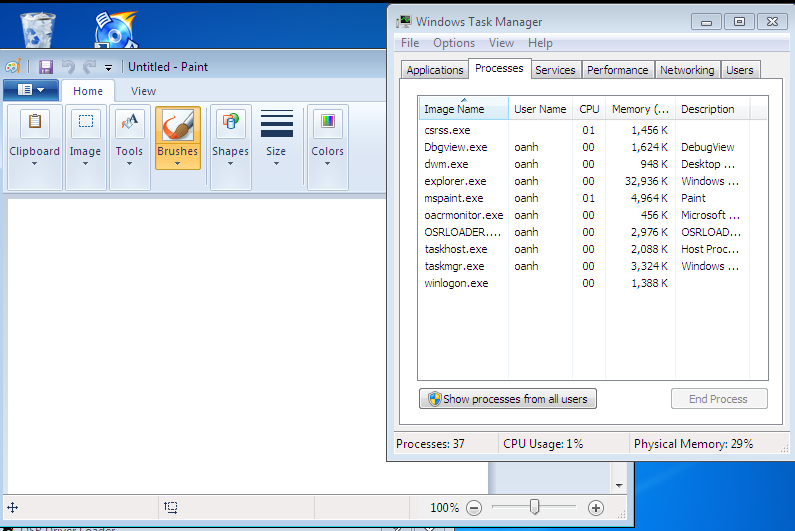
**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

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](https://uithcm-my.sharepoint.com/:v:/g/personal/21521253_ms_uit_edu_vn/EVq5GpQiXYlCocCbqLYgNbQB6EcIpEOWH8-XVUKsAyMYAA?e=qGpcUu&nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZy1MaW5rIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXcifX0%3D)

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



Đăng ký (Register Service) và chạy (Start Service) driver lên bằng ORS Driver Loader

A screenshot of a computer

Description automatically generated

Quan sát Task Manager. Lúc này mspaint đã được ẩn đi, trong khi chương trình Paint vẫn hoạt động bình thường.

A screenshot of a computer

Description automatically generated

Dừng (Stop Service) driver lại thì thấy mspaint có trong Task Manager.

Quan sát bằng DebugView.

A screenshot of a computer

Description automatically generated