TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN TPHCM

KHOA CÔNG NGHỆ THÔNG TIN

**\*\*\*---------------\*\*\***

**BÁO CÁO ĐỒ ÁN ĐỒ ÁN 3 (Đề 1)**

**SOFTWARE CRACKING**

*Giáo viên lý thuyết:*

* *Lê Quốc Hòa*
* *Chung Thuỳ Linh*
* *Lê Viết Long*

*Nhóm sinh viên thực hiện:*

* *Đặng Văn Hiển – 18120363*

**Mục lục**

1. **Thông tin nhóm 3**
   1. *Thông tin thành viên 3*
   2. *Bảng phân công công việc 3*
   3. *Mức độ hoàn thành công việc 3*

**1. Thông tin nhóm:**

**1.1: Thông tin thành viên:**

|  |  |  |
| --- | --- | --- |
| **MSSV** | **Họ Tên** | **Email** |
| 18120363 | Đặng Văn Hiển | 18120363@student.hcmus.edu.vn |
|  |  |  |

**1.2: Bảng phân công công việc:**

|  |  |  |
| --- | --- | --- |
| **MSSV** | **Họ Tên** | **Công việc** |
| 18120363 | Đặng Văn Hiển | Làm bài tập 1, 2, 3 |
|  |  |  |

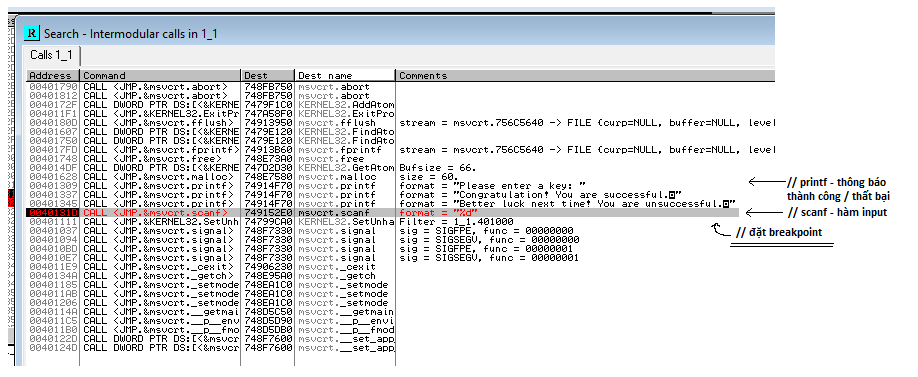
**1.3: Mức độ hoàn thành công việc:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Công việc** | | **Mức độ hoàn thành** | **Ghi chú** |
| Câu 1 | Nhập vào mảng số nguyên. | 100% |  |
| Xuất ra các phần tử. | 100% |  |
| Tính tổng các phần tử. | 100% |  |
| Liệt kê các phần tử là số nguyên tố. | 100% |  |
| Tìm max. | 100% |  |
| Tìm phần tử có giá trị x trong mảng. | 100% |  |
| Thoát chương trình | 100% |  |
| Các chức năng viết theo dạng hàm con. | 100% |  |
| Viết báo cáo cho câu 1 | 100% |  |
| Câu 2 |  | 100% |  |
|  | 100% |  |
|  | 100% |  |
|  | 100% |  |
|  | 100% |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**2. Bài tập 1:**

**2.1. Tìm đoạn code liên quan:**

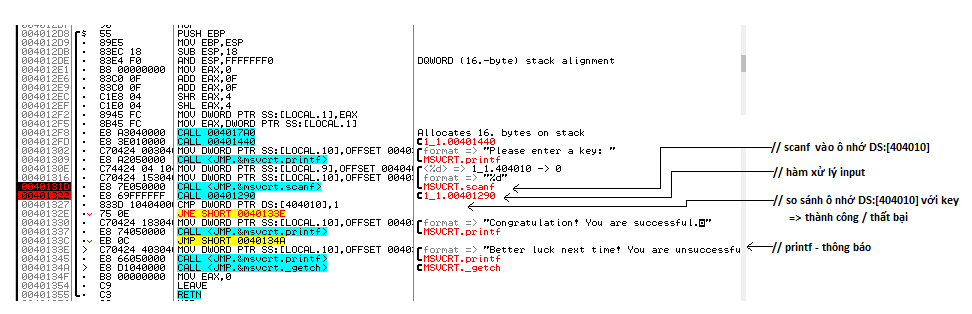
-Vào Intermodular calls để tìm input trong các hàm được gọi.



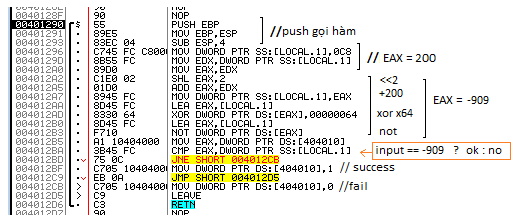
**2.2.Tìm hàm xử lý key:**

-F9 run debug đến breakpoint, ta theo dõi những hàm được gọi trước khi đến thông báo :

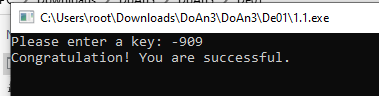
+ CALL 00401290

****

\* **Step into F7 vào CALL 00401290:**

**Sau khi phân tích hàm 00401290 ta => key = -909**

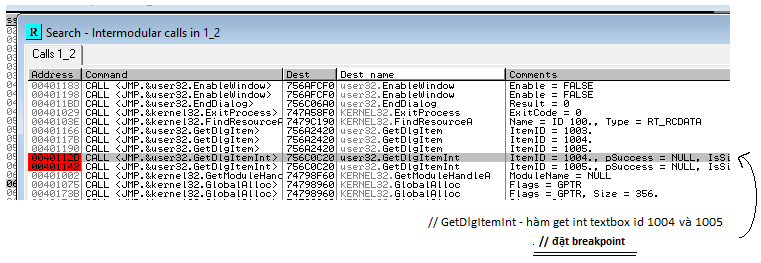
**2.3 Nhập key kiểm chứng:**



**3. Bài tập 2:**

**3.1. Tìm đoạn code liên quan:**

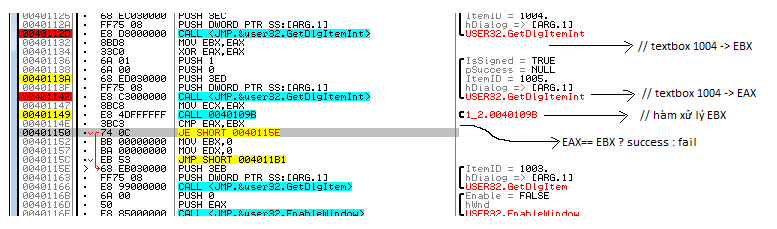
-Vào Intermodular calls để tìm input trong các hàm được gọi.

****

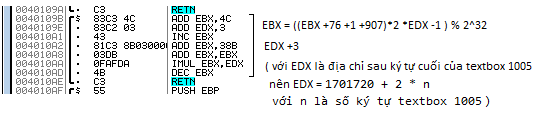
**3.2.Tìm hàm xử lý key:**

-F9 run debug đến breakpoint sau khi theo dõi luồng xử ký với key fail EAX==EBX thì success :

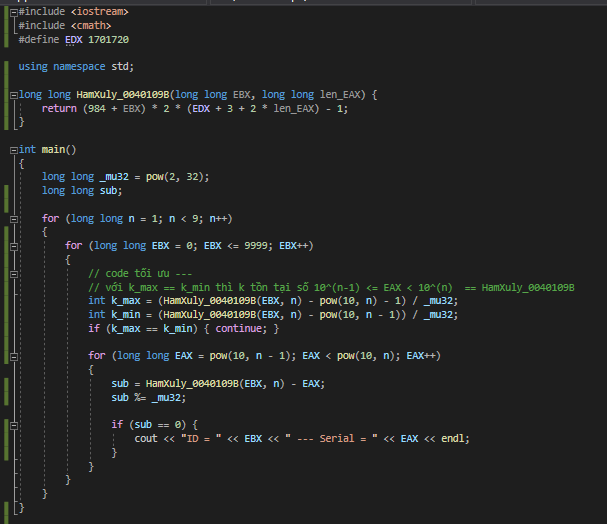
+ CALL 0040109B



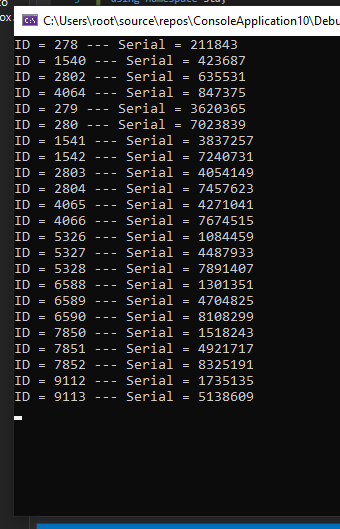
\* **Step into F7 vào CALL 0040109B:**

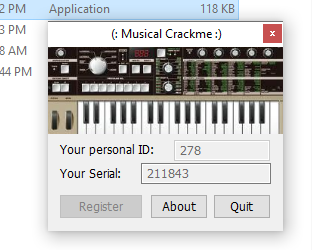
****

**Từ đó ta viết Keygen sao cho EBX (textbox 1004 qua xử lý ) == EAX (textbox 1005)**



**Với %=\_mu32 là khi phép nhân EAX nhận phần 32 bit bé .**

**3.3 Chạy Keygen và nhập key kiểm chứng:**



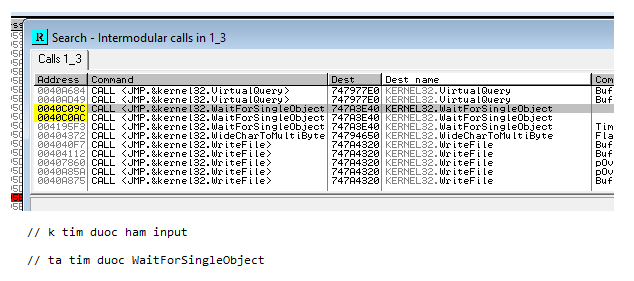
**4. Tham khảo:**

Tài liệu hướng dẫn trên moodle

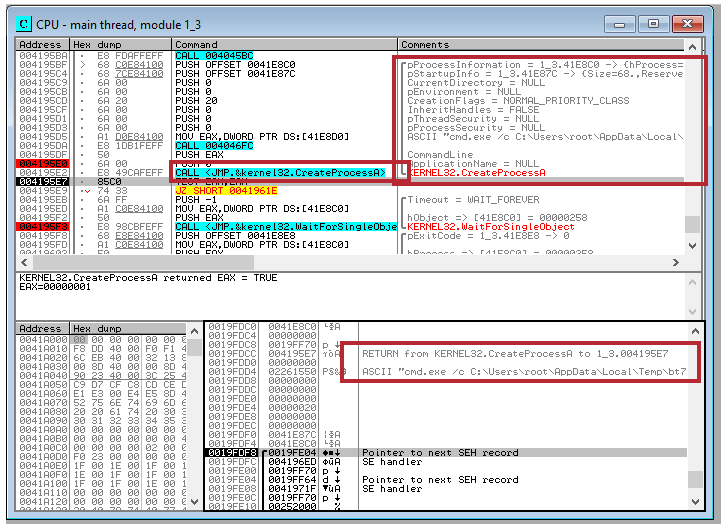
**Một đoạn nhạc không rõ nguồn gốc đă được phát … ♫♪♪~**

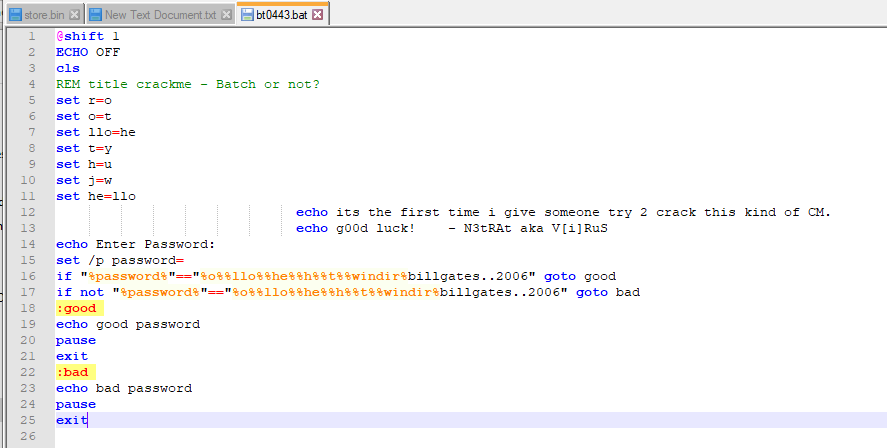
**4. Bài tập 3:**

**4.1. Tìm đoạn code liên quan:**



Và theo bộ nhớ Stack ta thấy chương trình có gọi tiến trình bằng lệnh cmd

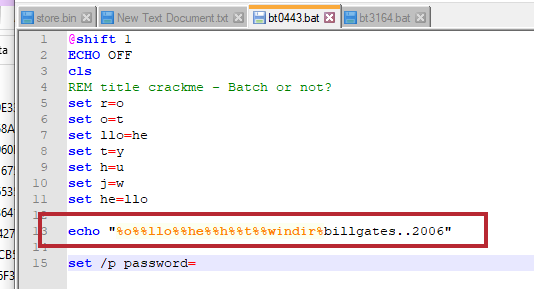
cmd.exe /c C:\Users\root\AppData\Local\Temp\bt6426.bat “C:\Users\root\Downloads\DoAn3\DoAn3\De01\1.3.exe"

Truy cập file bat trên ..

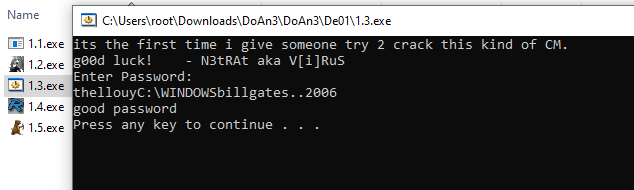
Theo các “biến” trong file batch ta có được mật khẩu phù hợp :

thellouyC:\WINDOWSbillgates..2006

(hoặc ta có thế echo mật khẩu ra trong 1 file bat trên)



**4.3 Nhập key kiểm chứng:**



**5. Bài tập 4:**

**5.1. Tìm đoạn code liên quan:**