**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

ĐẠI HỌC KHOA HỌC TỰ NHIÊN TPHCM

-----0-----

**BÁO CÁO ĐỒ ÁN**

Tên Đồ Án: Crack phần mềm

**Đề: 1**



Sinh viên thực hiện: Nguyễn Hữu Tú – 1612766

Nguyễn Anh Tuấn – 1612778

Câu 1.1:

* Dòng 0040112D là dòng lấy Personal ID(chỉ nhập số, không quá 4 số)

Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo với mức tin cậy rất cao

* Dòng 00401142 là dòng lấy số Serial (chỉ nhập số)

Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo với mức tin cậy rất cao

* Sau dòng 00401142 sẽ cập nhật giá trị thanh ghi EDX =00000000
* Dòng 00401149 dùng để biến đổi giá trị ID đầu vào( được lưu trong EBX)

EBX=[(EBX+4C+1+38B)\*2\*(EDX+3)]-1

Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo với mức tin cậy rất cao

Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo với mức tin cậy rất cao

* Dòng 0040114E để so sánh 2 thanh ghi EAX và EBX, nếu bằng sẽ nhảy đến dòng 0040115E, ngược lại sẽ tiếp tục đến dòng lệnh tiếp theo và nhảy đến 0040109B

Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo với mức tin cậy rất cao

* Dòng 0040115E: Tới được dòng lệnh này là có nghĩa serial và ID đã được chấp nhận và bắt đầu các câu lệnh xuất 1 đoạn nhạc ra.

Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo với mức tin cậy rất cao

* Dòng 0040109B: Tới dòng này có nghĩa là ID và số Serial không được chấp nhận, tiến hành thu hồi bộ nhớ và kết thúc chương trình.

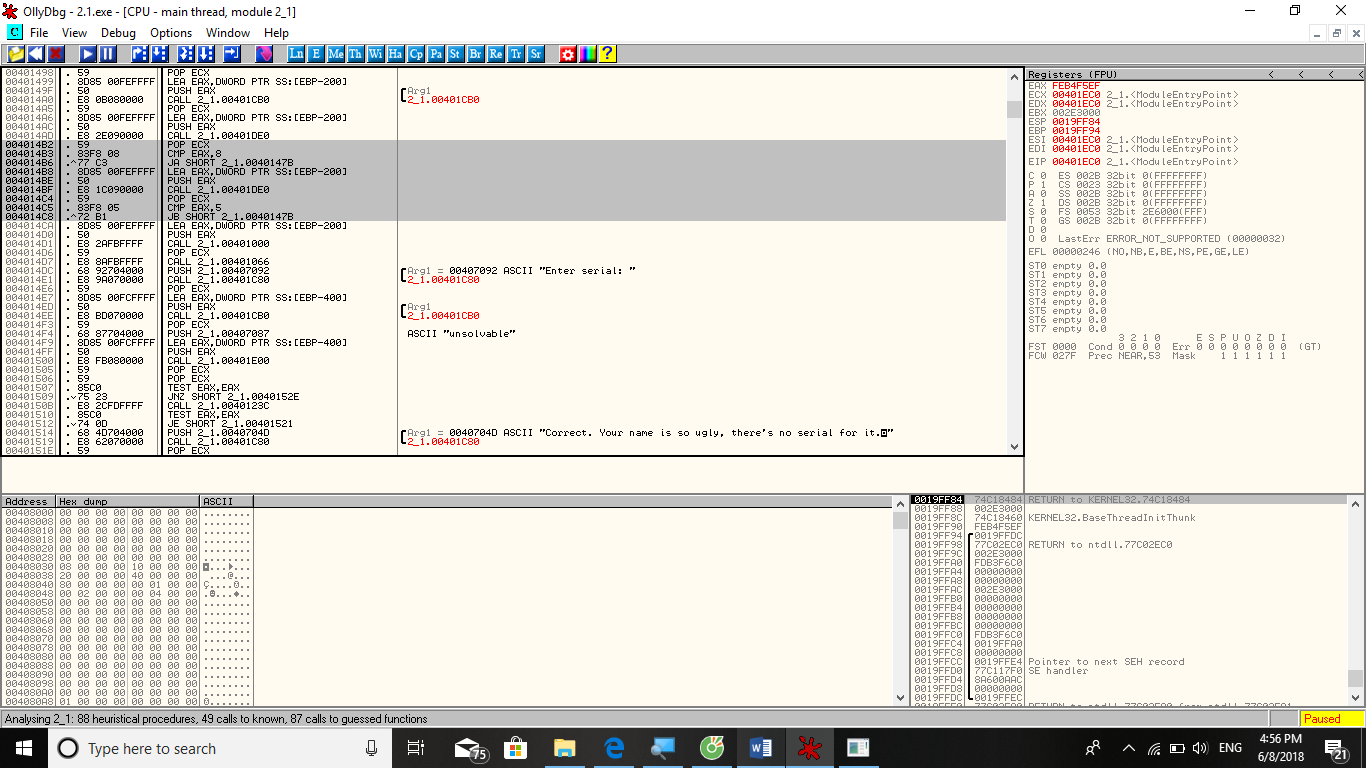
Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo với mức tin cậy rất cao

* Key ví dụ: Id: 1024; serial: 12047

Câu 2.1:

* Dòng 0040149F: Nhập username và lưu tại EAX
* Dòng 004014AC: đẩy username vào stack
* Dòng 004014AD: gọi hàm tính chiều dài username
* Dòng 004014B3 và 004014C5 để kiểm tra chiều dài nằm trong khoảng từ 5 đến 8, nếu không thì yêu cầu nhập lại.



* Dòng 004014EE để nhập số serial và lưu vào thanh ghi EAX
* Dòng 004014F4 để lưu chuỗi “unsolvable” vào stack
* Dòng 004014FF đẩy số serial vào stack
* Dòng 00401500 để gọi hàm kiểm tra key, nó sẽ nhảy tới địa chỉ 00401E00
* Dòng 00401E01 và 00401E05 :lấy số serial lưu vào EBX, lưu chuỗi “unsolvable” vào thanh ghi ECX.
* Hàm kiểm tra Key tại 00401E00: kiểm tra từng kí tứ của số serial có giống với chuỗi “unsolvable” không, nếu có thì EAX=1, ngược lại bằng 0

Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo với mức tin cậy rất cao

* Dòng 00401507: Kiểm tra EAX có bằng 0 hay không, nếu có thì nhảy tới 0040152E để xuất thông báo sai và yêu cầu nhập lại; ngược lại thì không nhảy mà tiếp tục thực hiện lệnh tiếp theo để xuất ra thông báo Thành công.