BMMMT&HT – Khoa CNTT

**LAB 3**

**Fuzzing - Reverse Engineering - Cryptography**

Họ tên và MSSV: Trần Lệ Uyên - 1050080165

Học phần: …………….

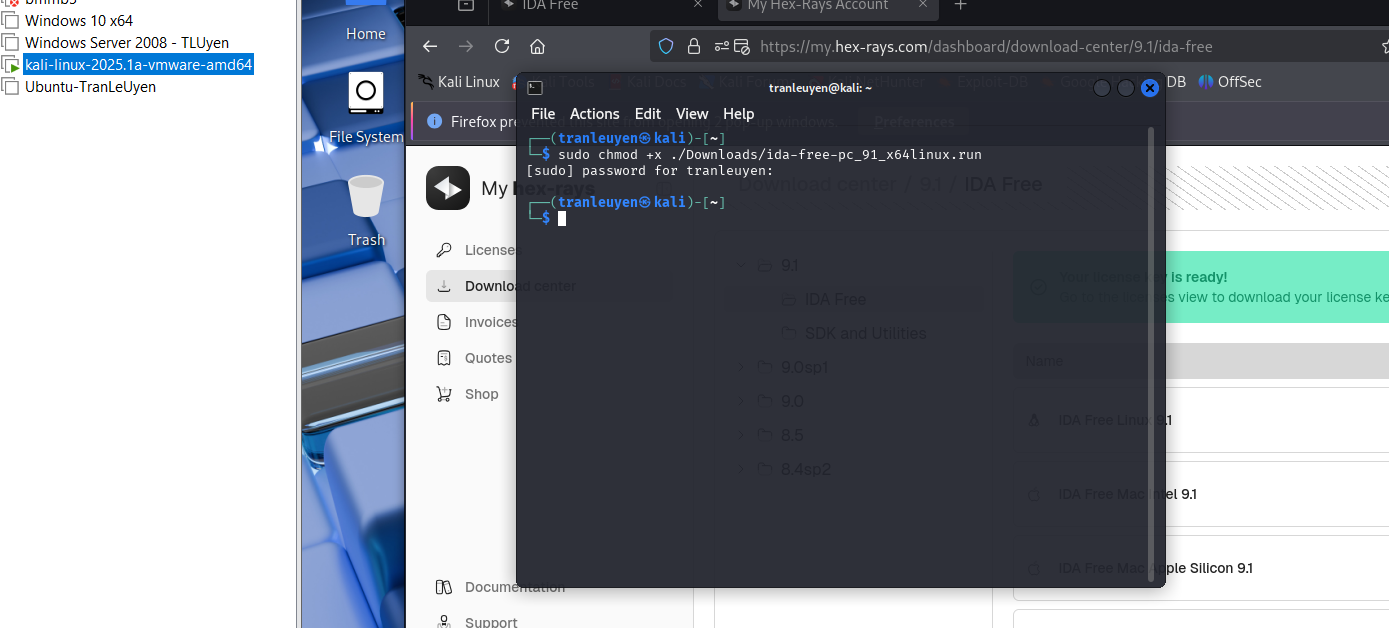
**Câu 1: Thực hiện kỹ thuật Reverse Engineering với công cụ IDA Free**

1.1. Cài đặt IDA Free vào Kali Linux. Tải file cài đặt (ví dụ: idafree83\_linux.run):

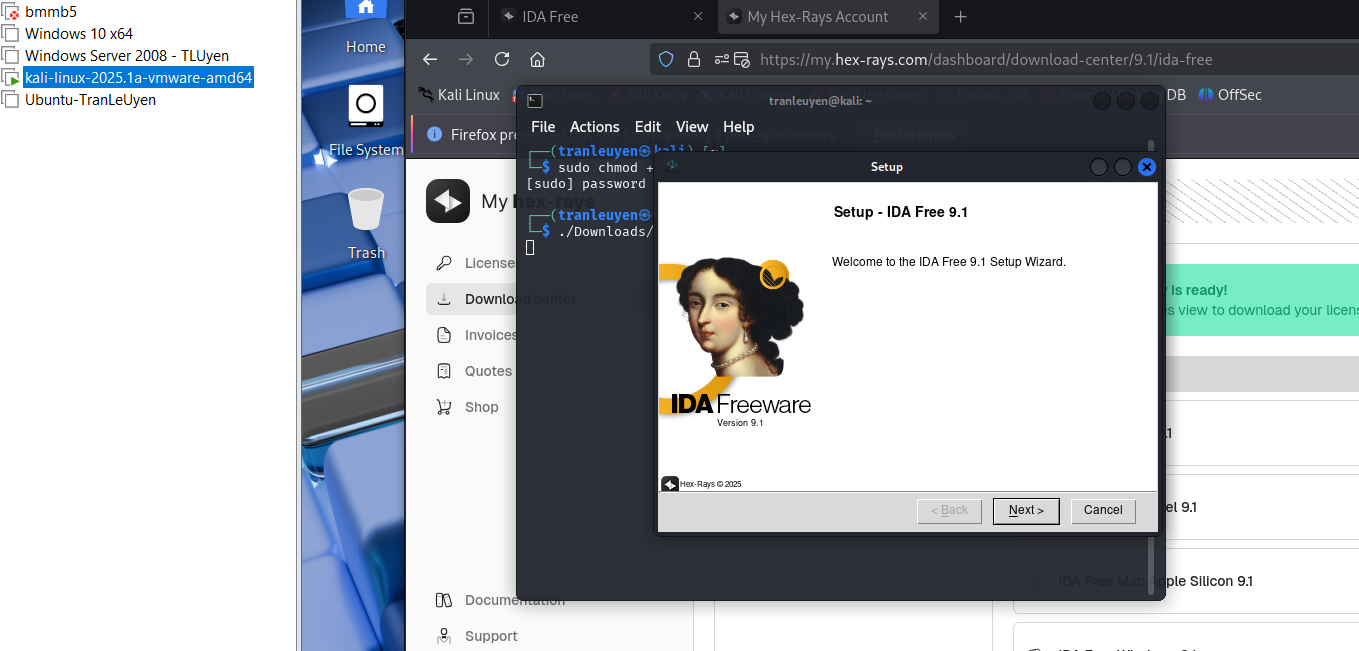
**$sudo chmod +x ./Downloads/idafree83\_linux.run**

**$./Downloads/idafree83\_linux.run**

➢ Tài và cài đạt IDA



➢ Thực hiện các bước theo yêu cầu. IDA Free sẽ được cài đặt ở thư mục cá nhân của người dùng.



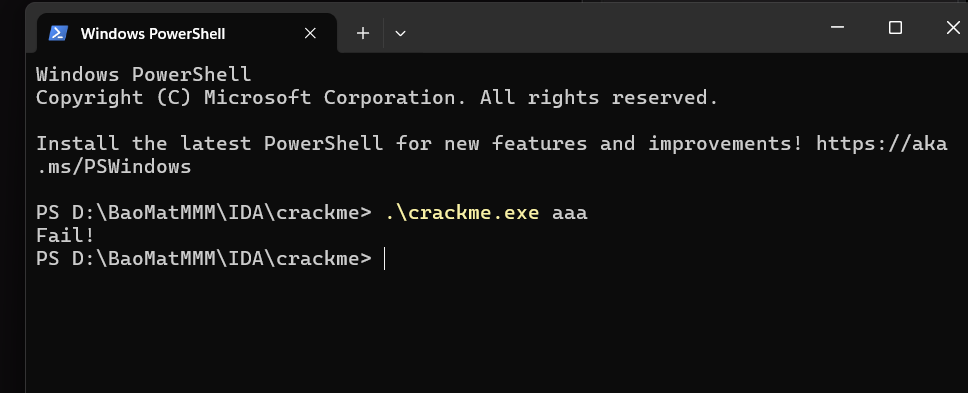
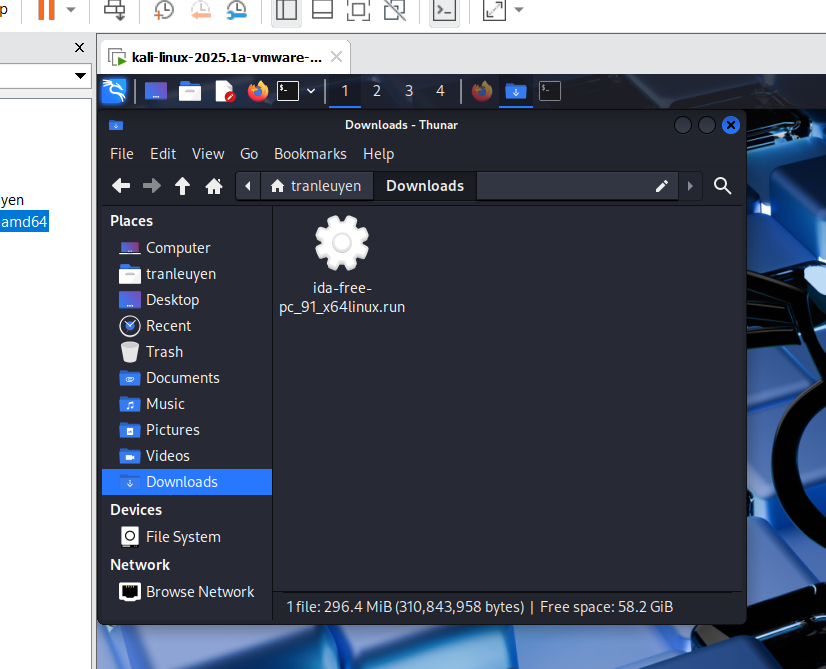
SVTH: ………………….. MSSV:

……………….

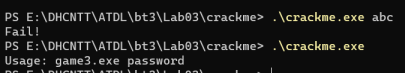
BMMMT&HT – Khoa CNTT

1.2. Nhấp vào link này 126 Proj 2x: Reverse Engineering with IDA Pro Freeware (10-40 pts.) tải các file về tạo file Lab03.zip.

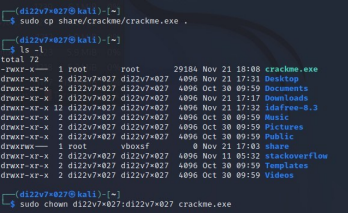
Trên máy Windows, tải file Lab03.zip. Giải nén sẽ được thư mục crackme chứa 02 file crackme.exe và msvcr100d.dll. Chạy file crackme.exe ở môi trường CMD với vài giá trị đầu vào khác nhau và xem kếtquả.



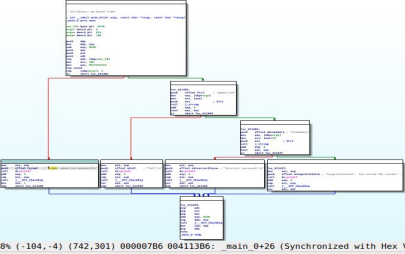
BMMMT&HT – Khoa CNTT

1.3. Di chuyển file crackme.exe vào máy ảo Kali Linux (sử dụng chức năng Shared Folders hoặc Drag and Drop). Chạy IDA Free và mở file crackme.exe trên môi trường IDA Free.

➢ **Dùng lệnh để copy file: $sudo cp share/crackme/crackme.exe .**

****

1.4. Trên thanh menu, sử dụng chức năng “Search, Text” tìm kiếm với từ khóa “usage”. Trên cửa sổ “IDA - View A” chọn “Fit window”. Chọn “Text view” hoặc “Graph view” để xem mã Assembly của chương trình.



SVTH: ………………….. MSSV: ……………….

BMMMT&HT – Khoa CNTT

1.5 Trên thanh menu, sử dụng chức năng “View, Sub view, Generate pseudo code” (F5) để sinh mã giả