Họ và Tên: Trầm Xuân Trọng

Lớp: 10ĐH\_CNPM1

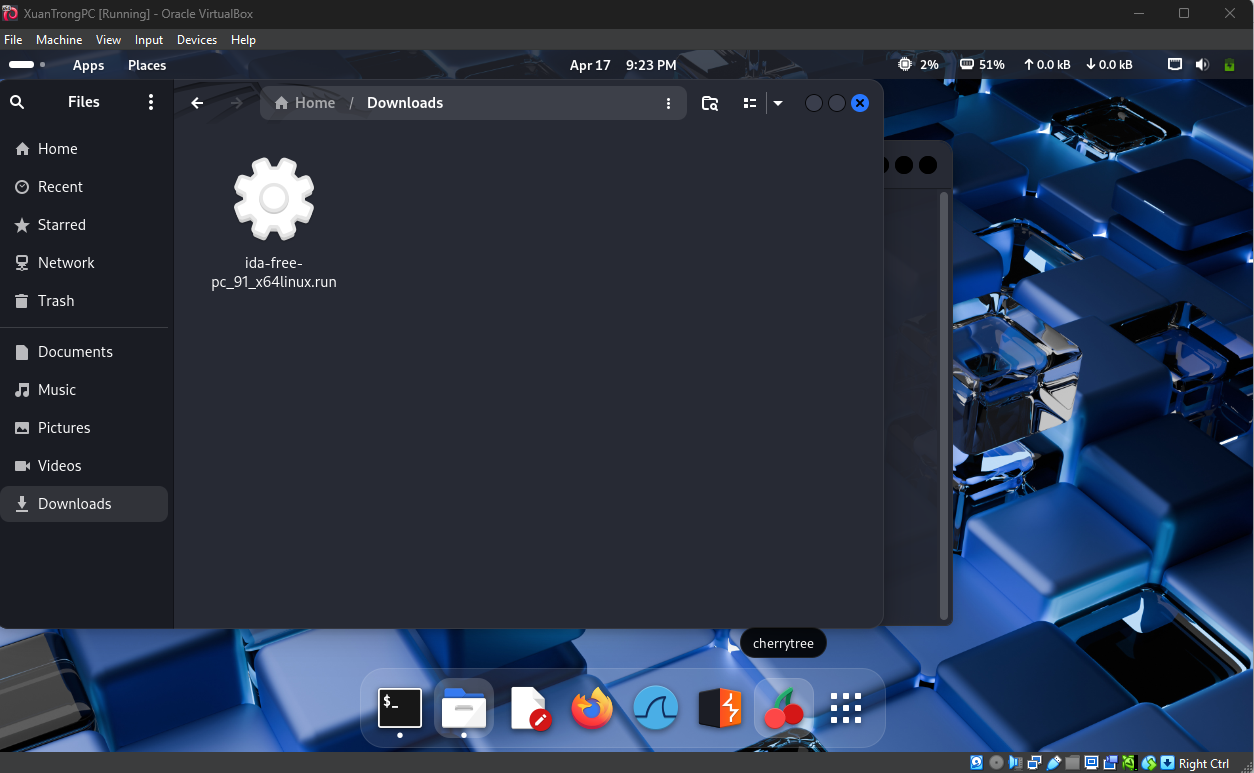
MSSV: 1050080081

**Lab 3**

**Fuzzing – Reverse Engineering – Cryptography**

Câu 1:

* 1. Cài đặt IDA Free

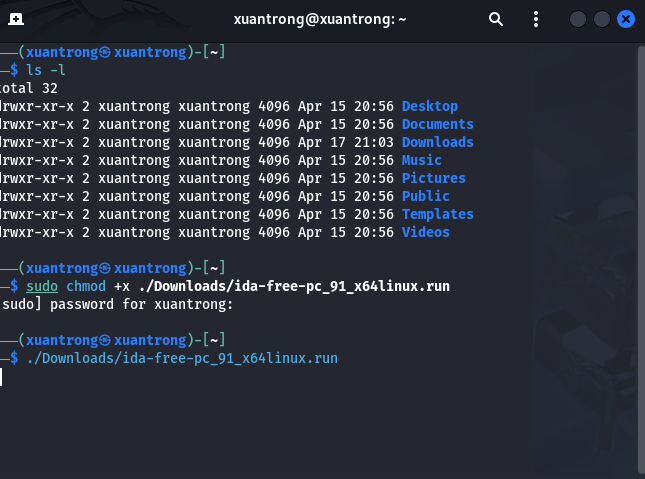


**$sudo chmod +x ./Downloads/ida-free-pc\_91\_x64linux.run**

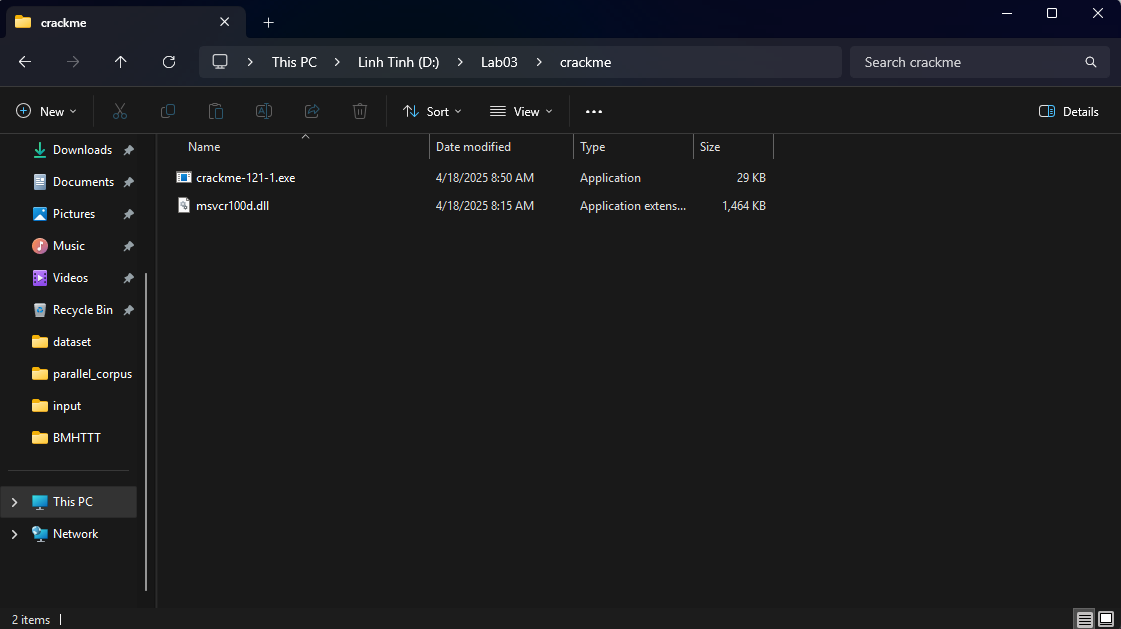
**$./Downloads/ ida-free-pc\_91\_x64linux.run**

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

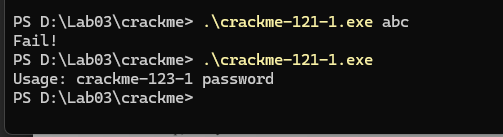
****



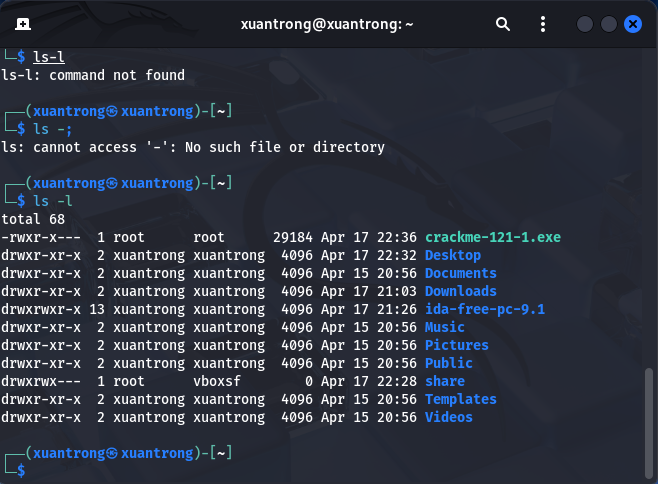
* 1. Thực hiện tải file theo yêu cầu



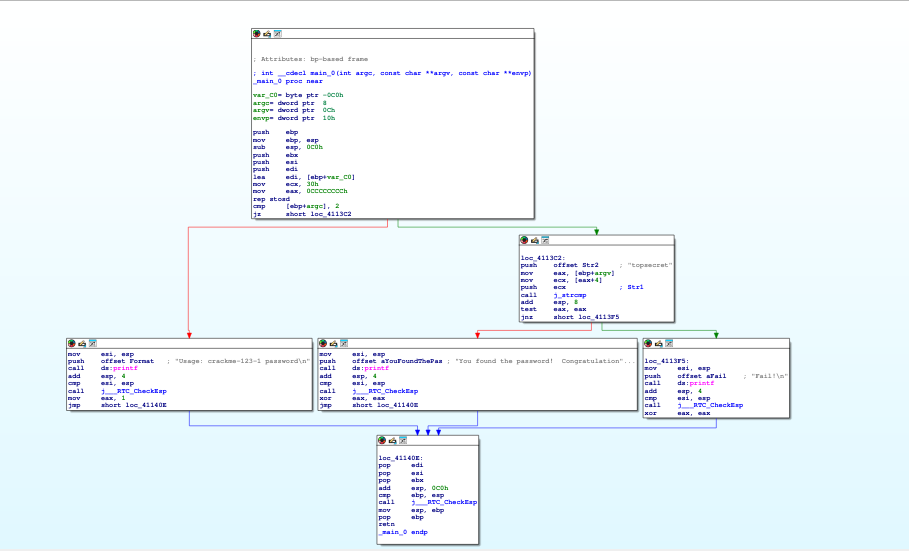
Chạy file crackme-121-1.exe bằng CMD với vài giá trị đầu vào để xem kết quả



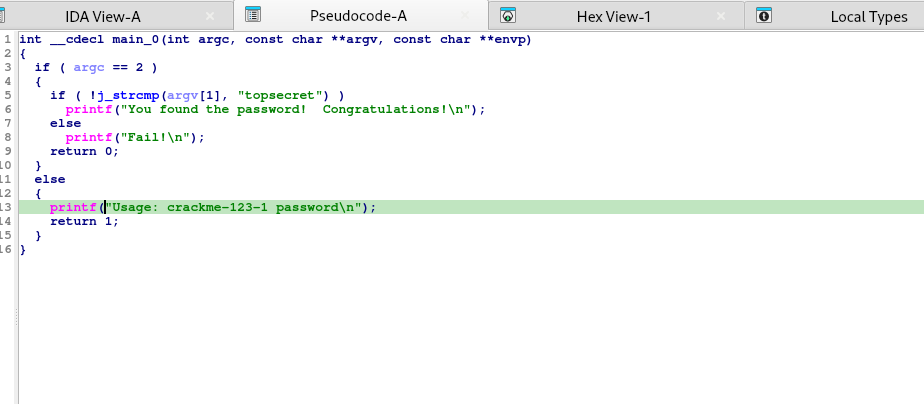
* 1. Di chuyển file crackme-121-1.exe vào máy ảo Kali Linux bằng Shared Foler. Chạy IDA Free và mở file crackme-121-1.exe trên môi trường IDA Free.
* Dùng lệnh để copy file: **$sudo cp share/crackme/crackme.exe. ( nếu dùng shared folder ).**



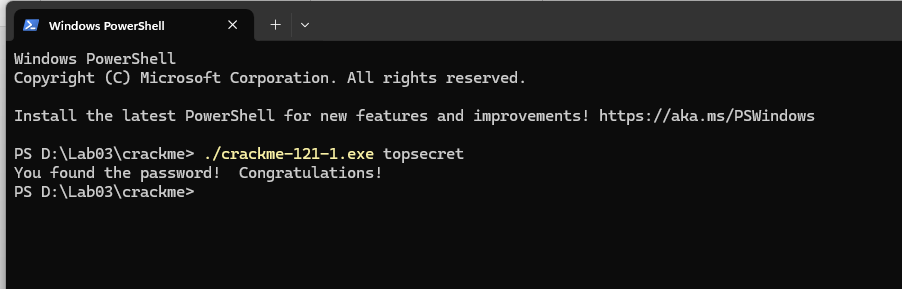
* 1. Nếu tải version 9 thì nhớ tải lisence key cho ứng dụng thì mới mở được. Trên thanh menu, sử dụng chức năng “Search, Text” tìm kiếm với từ khóa “usage”. Trên cửa sổ “IDA - View A” chọn “Fit window”. Chọn “Text view” hoặc “Graph view” để xem mã Assembly của chương trình.



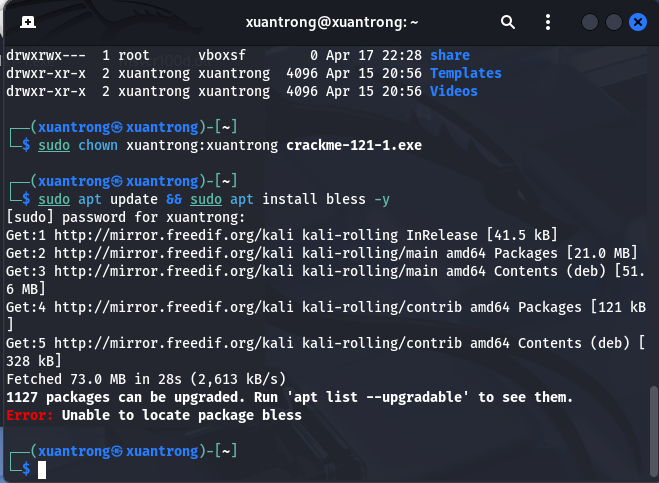
* 1. Trên thanh menu, sử dụng chức năng “View, Sub view, Generate pseudo code” (F5) để sinh mã giả của crackme.exe. Trên cửa sổ “Pseudocode - A”, sử dụng chức năng “Synchronize with” để đồng bộ với “IDA- View A” và “Hex - View 1”.



* 1. Phân tích mã giả của crackme-121-1.exe để chạy thông báo “You found the password! Congratulations” chạy file crackme-121-1.exe ở môi trường CMD của máy windows để thực hiện.



* 1. Cài đặt công cụ Bless hex editor vào Kali Linux:
* Cài đặt như sau: **$ sudo apt update && sudo apt install bless –y**



Gặp lỗi thì sủa như sau:

✓ B1: $**sudo nano /etc/apt/sources.list**

✓ B2: Xoá toàn bộ dữ liệu trong file

✓ B3: Copy đoạn mã bên dưới dán vào file -> Lưu lại

deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware

deb http://http.kali.org/kali kali-last-snapshot main contrib non-free non-free-

firmware

deb http://http.kali.org/kali kali-experimental main contrib non-free non-free-

firmware

deb http://http.kali.org/kali kali-bleeding-edge main contrib non-free non-free-

firmware

deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-

firmware

✓ B4: **$sudo apt-get upgrade**

✓ B5: **$sudo apt-get update**

✓ B6: **$sudo apt-get install checkinstall**

✓ B7: **$sudo apt install bless –y**

✓ B8: Sừ dụng lệnh **$bless** để kiểm tra cài đặt thành công chưa ?