LAB 3

Fuzzing - Reverse Engineering – Cryptography

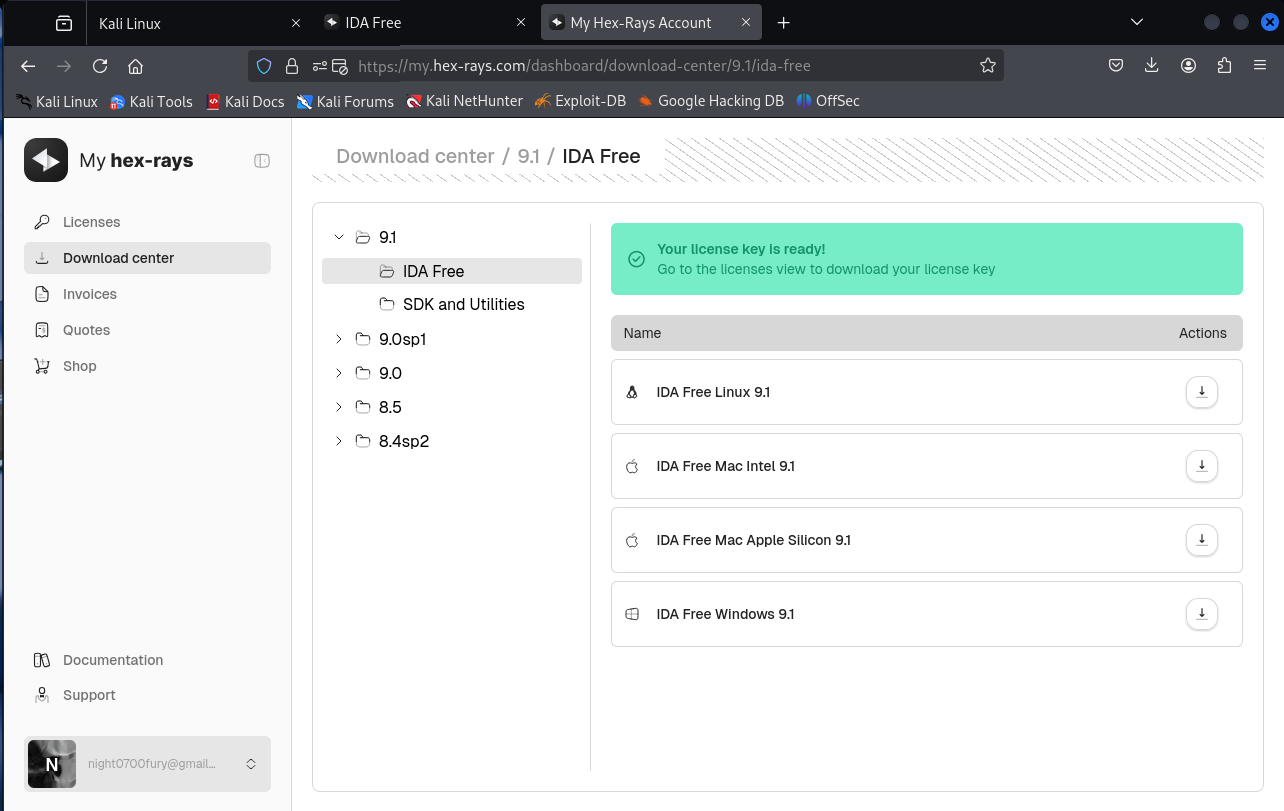
Họ tên: Trần Quốc Bảo

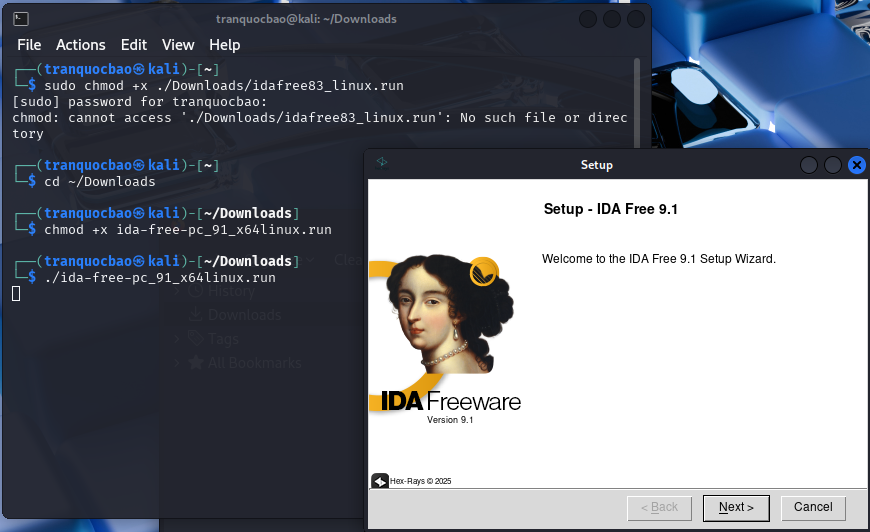
Mssv: 1050080129

Lớp: 10\_ĐH\_CNPM2

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

1.1 Cài đặt [IDA Free](https://hex-rays.com/ida-free/#download) vào Kali Linux. Tải file cài đặt





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

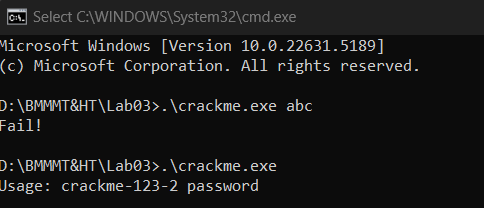
về tạo file Lab03.zip.

Trên máy Windows, tải file Lab03.zip. Giải nén sẽ được thư mục crackme chứa 02 file crackme.exe và

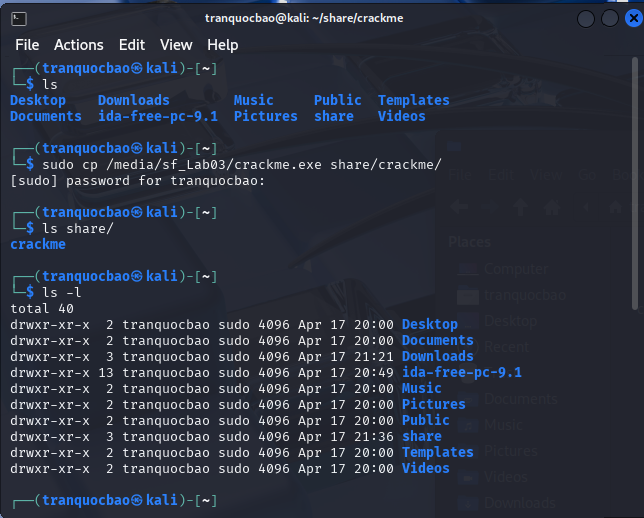
msvcr100d.dll. Chạy file crackme.exe ở môi trường CMD với vài giá trị đầu vào khác nhau và xem kếtquả.

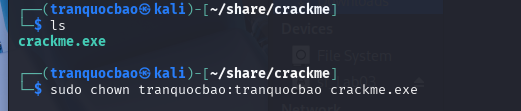


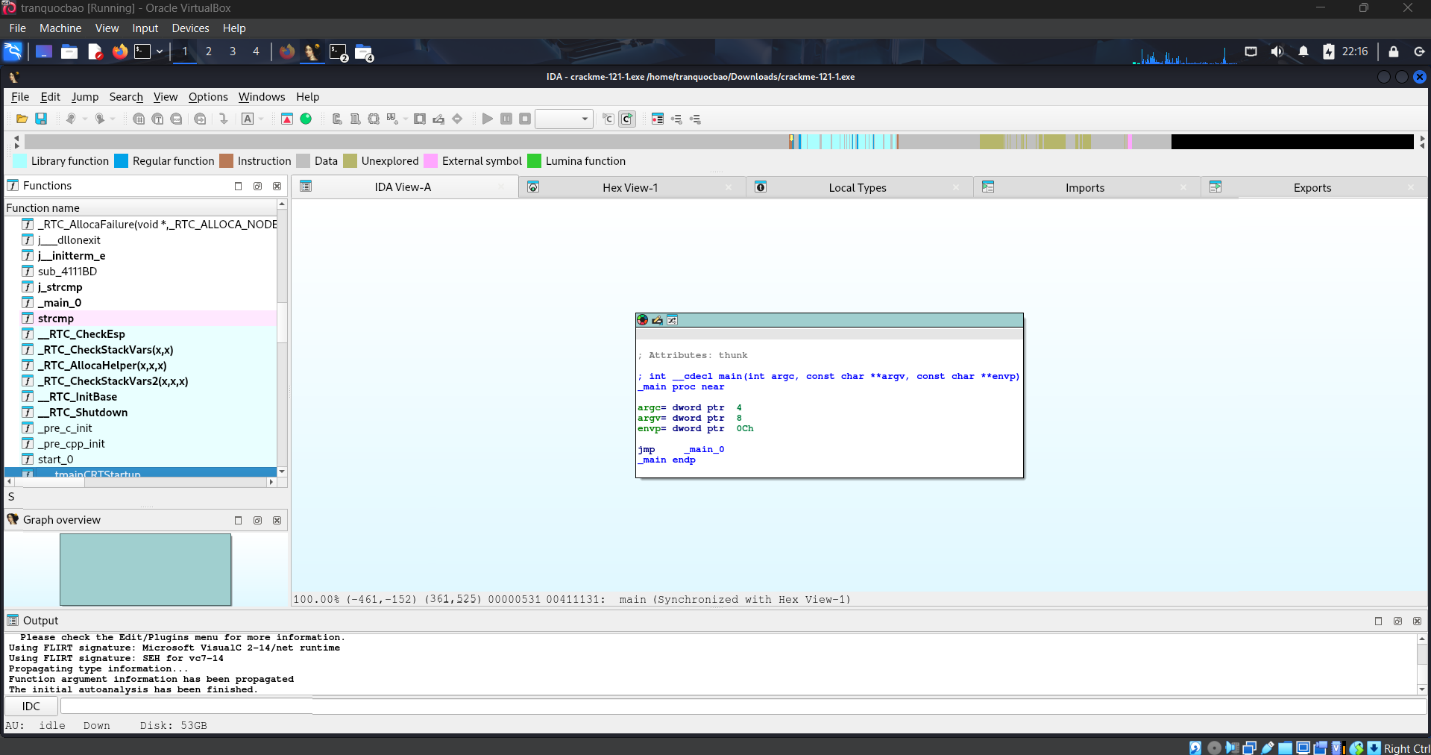




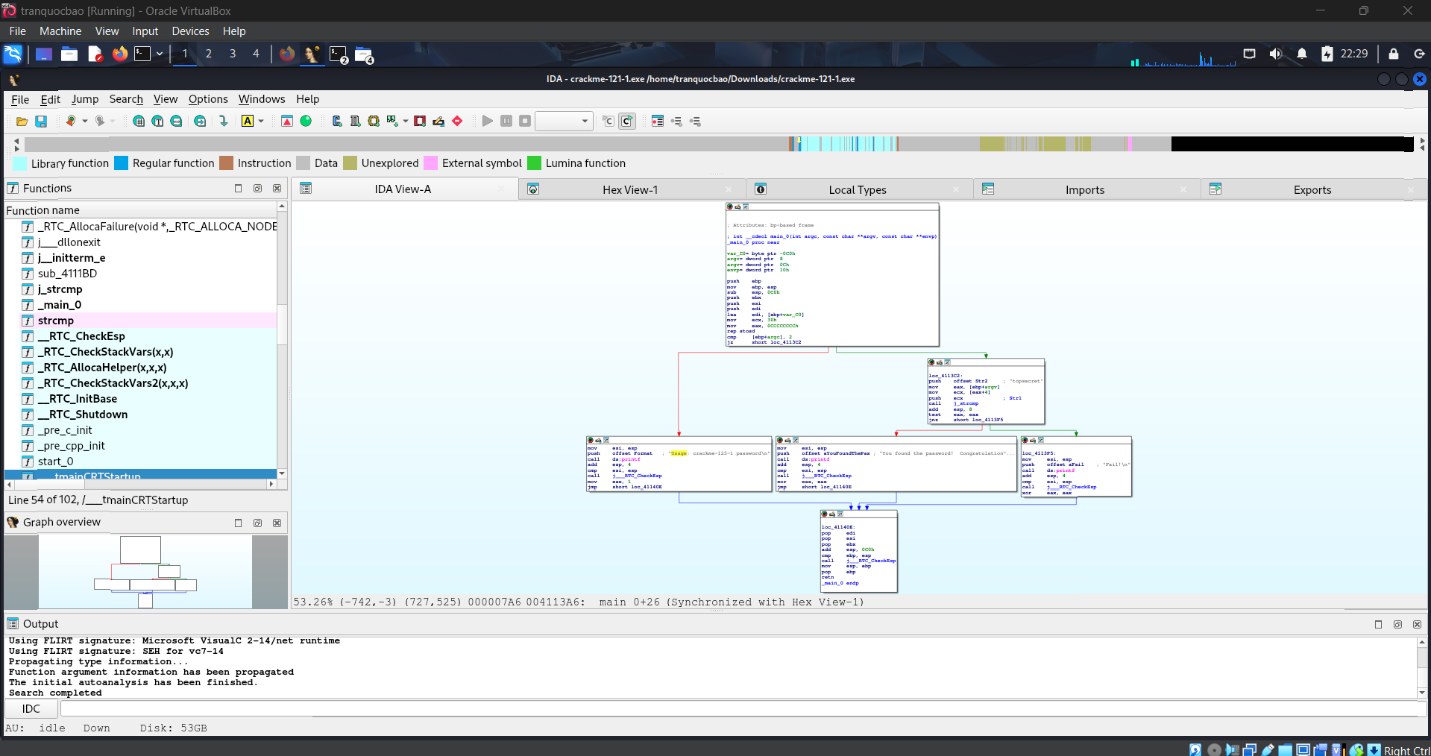
* 1. Di chuyển file crackme.exe vào máy ảo Kali Linux (sử dụng chức năng Shared Folders hoặc Drag and Drop). Chạy IDA Free và mở file crackme.exe trên môi trường IDA Free.

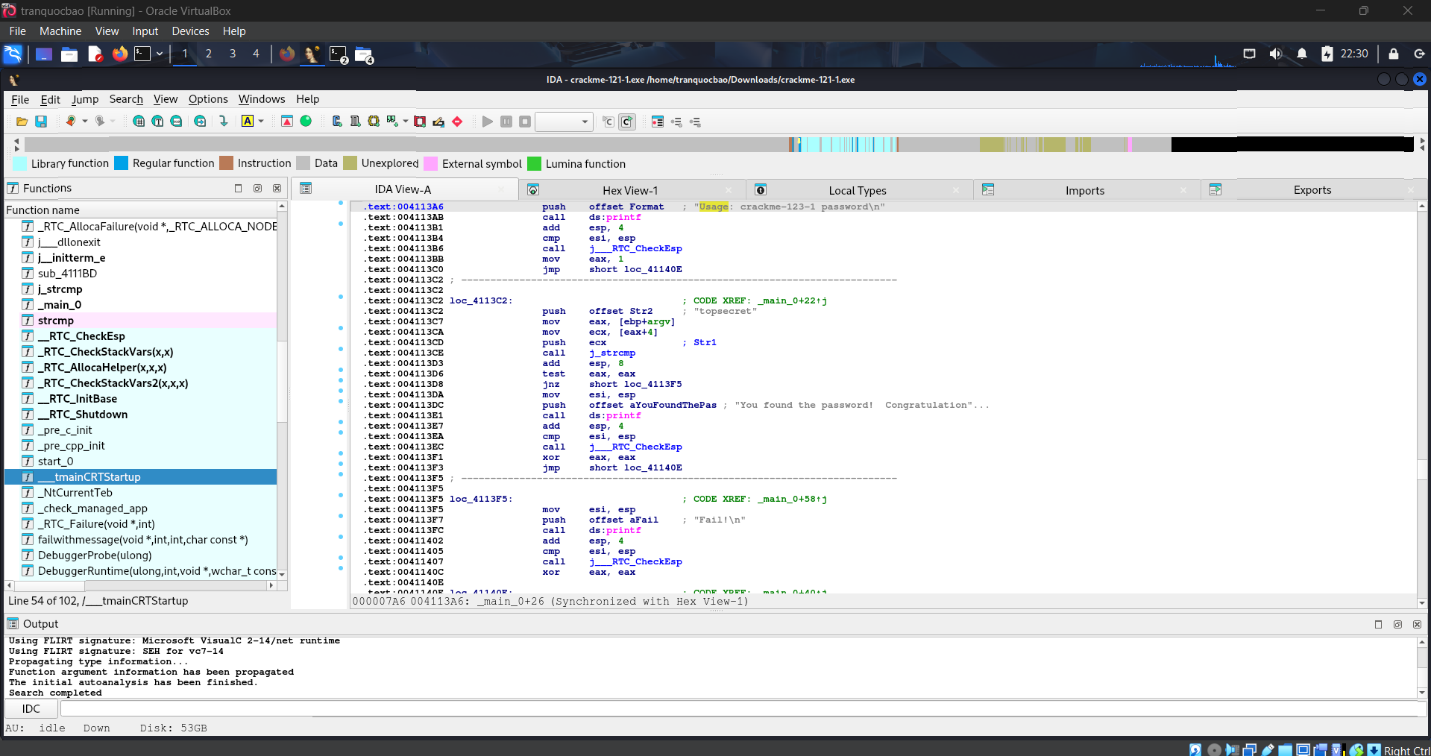






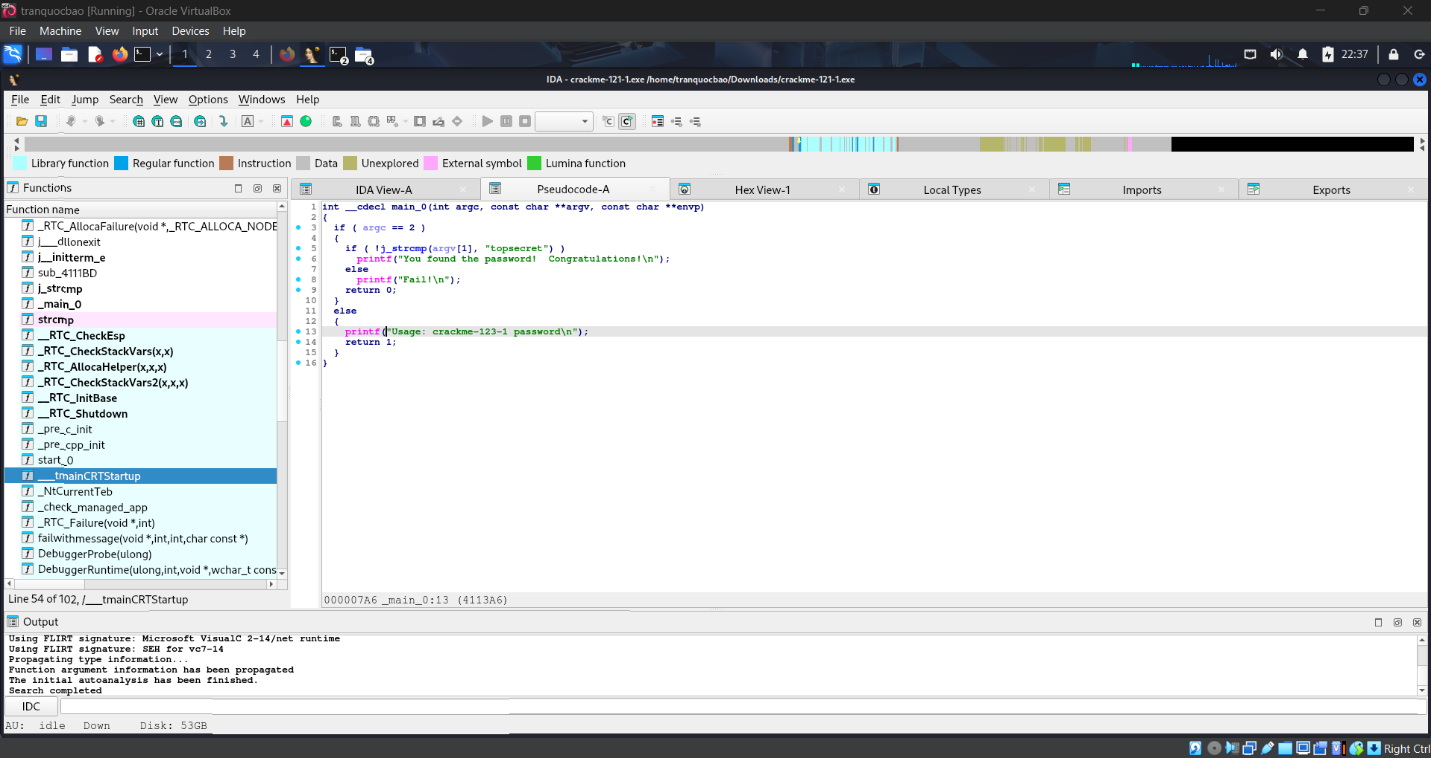
* 1. Trên thanh menu, sử dụng chức năng “Search, Text” tìm kiếm với từ khóa “usage”. Trên cửa sổ “IDA - View A” chọn “Fit window”. Chọn “Text view” hoặc “Graph view” để xem mã Assembly của chương trình.



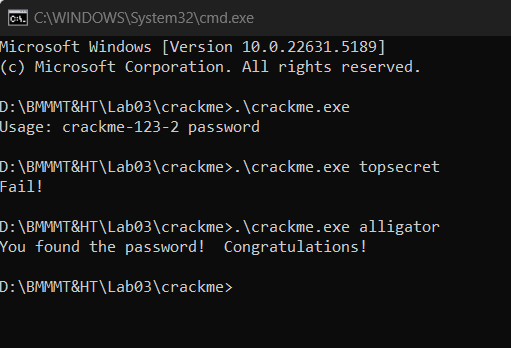


* 1. Trên thanh menu, sử dụng chức năng “View, Sub view, Generate pseudo code” (F5) để sinh mã giả của crackme.exe. Trên cửa sổ “Pseudocode - A”, sử dụng chức năng “Synchronize with” để đồng bộ với “IDA

- View A” và “Hex - View 1”.

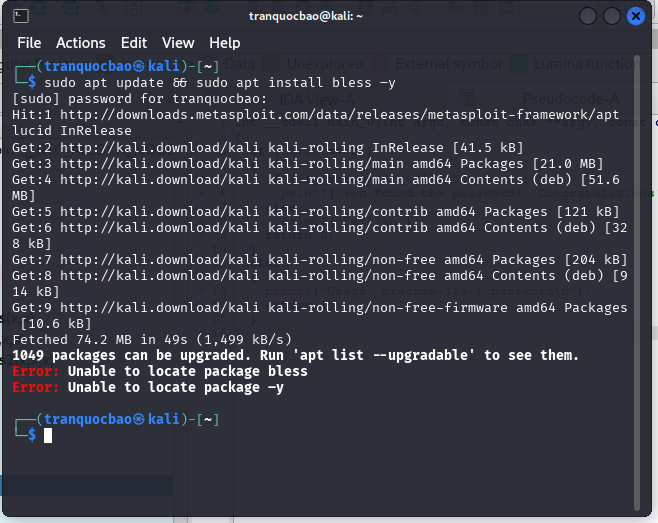


* 1. Phân tích mã giả của crackme.exe để có thể chạy chương trình in ra thông báo "Congratulations! You solved the crackme puzzle!”. Chạy file crackme.exe ở môi trường CMD của máy Windows in ra thông báo trên.



* 1. Cài đặt công cụ Bless hex editor vào Kali Linux:
     + Cài đặt Bless

# $ sudo apt update && sudo apt install bless –y



* + - Cách xử lý lỗi khi cài bless

# 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

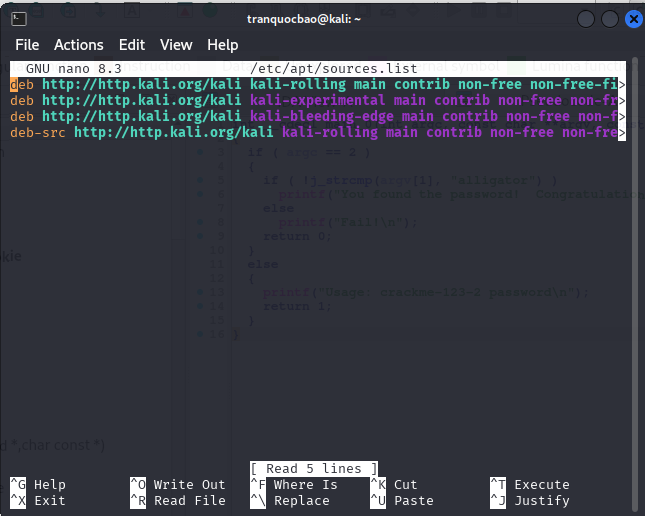
deb <http://http.kali.org/kali> kali-experimental main contrib non-free non-free- firmware

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

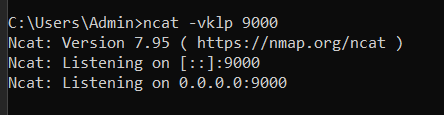
* + - * B4: **$sudo apt-get upgrade**
      * B5: **$sudo apt-get update**
      * B6: **$sudo apt-get install checkinstall**
      * B7: **$sudo apt install bless –y**
      * B8: Sừ dụng lệnh **$bless** để kiểm tra cài đặt thành công chưa ?





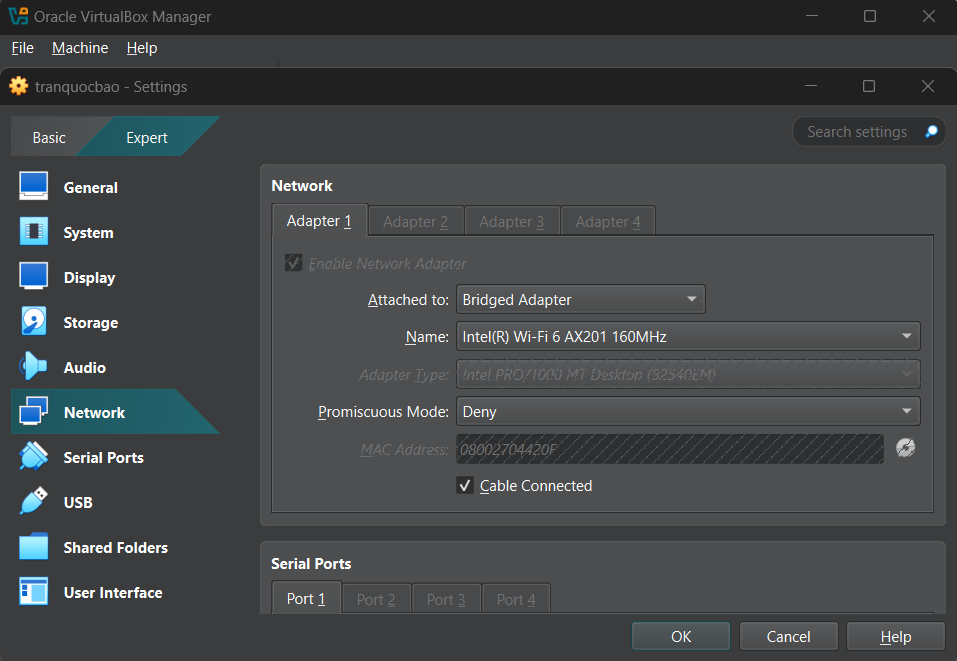
# Câu 2: Thực hiện kỹ thuật Fuzzing với công cụ Spike

Cài đặt công cụ [nmap (Zenmap)](https://nmap.org/download.html#windows) trên máy Windows

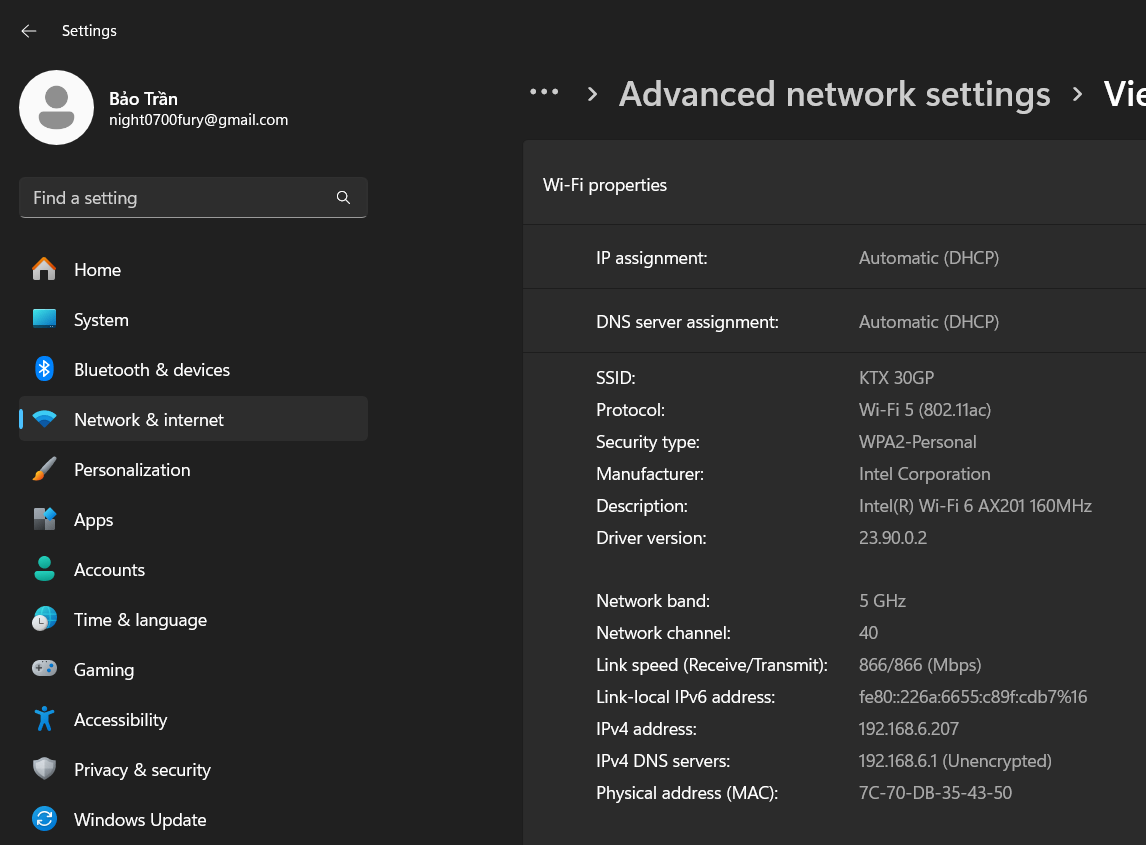


* + Thay đổi cấu hình mạng của máy ảo Kali Linux sao cho có thể giao tiếp mạng tới máy

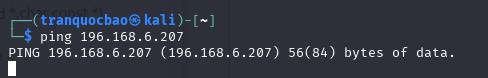
Windows (Sử dụng mạng Internet được chia sẻ từ điện thoại )



* + IP của máy Windows 192.168.188.177



* + Kiểm tra ping 192.168.6.207

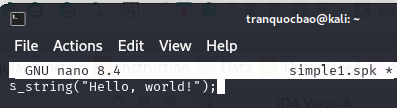


* Tạo file simple1.spk với nội dung bên dưới:
  + $nano simple1.spk

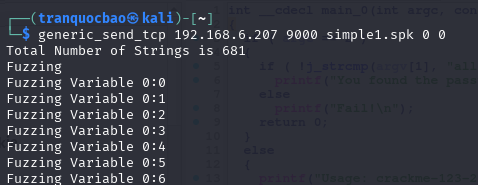


* + Nội dung file

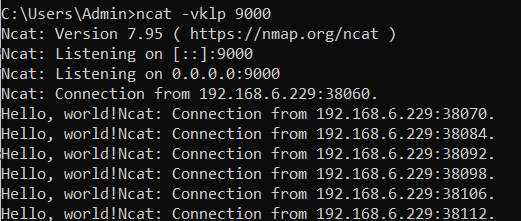
s\_string("Hello, world!");



* Thực hiện lệnh sau để fuzzing dịch vụ Netcat. Quan sát kết quả dịch vụ Netcat nhận được.
  + $ generic\_send\_tcp 192.168.188.177 9000 simple1.spk 0 0



* + Kết quả dịch vụ Netcat



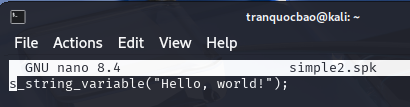
* + Tạo file simple2.spk với nội dung bên dưới:

# $nano simple2.spk

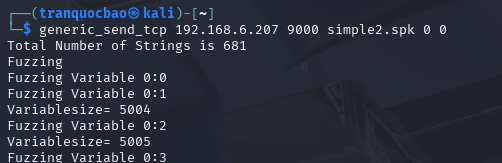


* + # Nội dung file

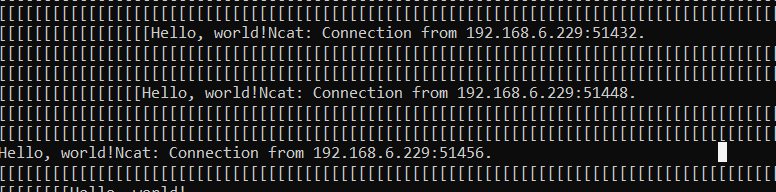
s\_string\_variable("Hello, world!");



* Thực hiện lệnh sau để fuzzing dịch vụ Netcat. Quan sát kết quả dịch vụ Netcat nhận được.
  + $ generic\_send\_tcp 192.168.188.177 9000 simple2.spk 0 0



* + Kết quả dịch vụ Netcat

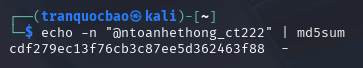


# Câu 3: Giải thuật băm và tấn công mật khẩu

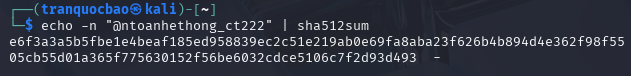
* 1. Tìm giá trị băm của chuỗi "@ntoanhethong\_ct222" sử dụng giải thuật MD5 và SHA512 sử dụng

công cụ md5sum và sha512sum:

# $ echo -n "@ntoanhethong\_ct222" | md5sum

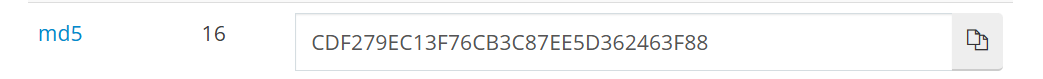


* + - **$ echo -n "@ntoanhethong\_ct222" | sha512sum**



* + - Sử dụng một trang web online cho phép thực hiện giải thuật băm, ví dụ

:<https://www.pelock.com/products/hash-calculator> để kiểm tra kết quả.



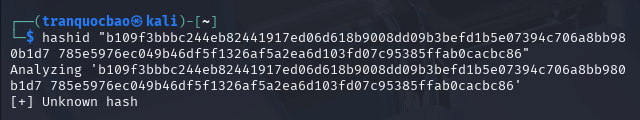


* 1. Sử dụng công cụ john và hashcat để dịch ngược giá trị băm "b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46 df5f1326af5a2ea6d103fd07c95385ffab0cacbc86"

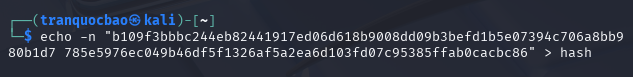
# Xác định giải thuật băm

* + - **$ hashid**

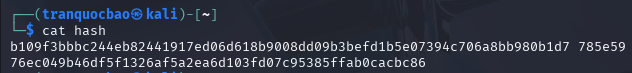
**"b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7 785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86"**



* + - $ **echo -n "b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7 785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86" > hash**

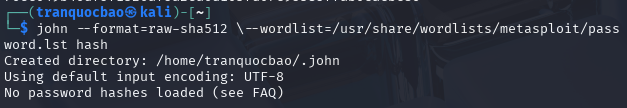


* + - **Hiển thị nội dung: $ cat hash**



* + - # Sử dụng John the Ripper

# $john --format=raw-sha512 \--wordlist=/usr/share/wordlists/metasploit/password.lst hash

\

* + - # Sử dụng hashcat

# $hashcat -a 0 -m 1700 ./hash /usr/share/wordlists/metasploit/password.lst

