Họ tên : Trần Thái Thắng

Lớp : CNPM3

**1️. Keylogger là gì?**

Keylogger (Keystroke Logger) là một loại phần mềm hoặc phần cứng có khả năng ghi lại mọi thao tác bàn phím của người dùng mà không cần sự cho phép. Keylogger thường được sử dụng với nhiều mục đích khác nhau, từ hợp pháp đến bất hợp pháp:

Ứng dụng hợp pháp:

Doanh nghiệp giám sát hoạt động nhân viên.

Phụ huynh theo dõi con cái.

Người dùng cá nhân sử dụng để tự động lưu lại dữ liệu nhập trên máy tính.

Ứng dụng bất hợp pháp:

Hacker đánh cắp thông tin đăng nhập, mật khẩu, thông tin ngân hàng.

Theo dõi hoạt động của người dùng mà không có sự đồng ý.

Cài đặt trong các cuộc tấn công mạng để lấy thông tin nhạy cảm.

**2️.Phân biệt các loại Keylogger**

Keylogger có thể được chia thành hai loại chính:

| Loại Keylogger | Mô tả | Cách thức hoạt động | Ví dụ thực tế |
| --- | --- | --- | --- |
| Hardware Keylogger | Thiết bị vật lý gắn vào máy tính để ghi lại thao tác bàn phím. | Gắn trực tiếp vào cổng USB hoặc giữa bàn phím và máy tính để chặn tín hiệu. | Thiết bị nhỏ gọn cắm vào cổng USB, Keylogger Bluetooth. |
| Software Keylogger | Chương trình chạy ẩn trên hệ điều hành, ghi lại các thao tác bàn phím. | Cài đặt vào hệ thống và ghi lại dữ liệu gõ phím, sau đó gửi về máy chủ hoặc lưu trữ cục bộ. | Trojan Keylogger, Malware Keylogger, Keylogger trong trình duyệt. |

**3️.Cách sử dụng Software Keylogger để nghiên cứu**

**Trên máy tính (Windows/Linux/Mac)**

Một số Keylogger phổ biến có thể được cài đặt để nghiên cứu:

Revealer Keylogger (Windows)

Spyrix Free Keylogger (Windows, Mac)

Logkeys (Linux)

**Cách hoạt động:**

Ghi lại các thao tác bàn phím.

Ẩn trong hệ thống (hoặc chạy dưới dạng dịch vụ).

Gửi dữ liệu về email hoặc lưu trữ cục bộ.

**Trên điện thoại (Android/iOS)**

Một số ứng dụng theo dõi hoạt động bàn phím trên điện thoại:

iKeyMonitor

Spyic

Hoverwatch

**Cách hoạt động:**

Ghi lại nội dung nhập trên bàn phím điện thoại.

Theo dõi hoạt động ứng dụng, tin nhắn.

Gửi dữ liệu về máy chủ của hacker (nếu bị cài đặt trái phép).

**4️. Cách phòng tránh Keylogger**

🔐 Để bảo vệ máy tính và điện thoại khỏi Keylogger, bạn có thể thực hiện các biện pháp sau:

**Phòng tránh Software Keylogger:**

Sử dụng phần mềm diệt virus: Windows Defender, Malwarebytes, Kaspersky...

Không tải phần mềm không rõ nguồn gốc: Tránh tải phần mềm lậu, ứng dụng crack.

Sử dụng bàn phím ảo: Giúp tránh bị ghi lại khi nhập thông tin nhạy cảm.

Kiểm tra Task Manager (Windows) hoặc Activity Monitor (Mac): Tìm các tiến trình đáng ngờ.

Dùng trình quản lý mật khẩu: Giảm thiểu việc nhập mật khẩu bằng tay.

**Phòng tránh Hardware Keylogger:**

Kiểm tra cổng kết nối USB: Đảm bảo không có thiết bị lạ cắm vào.

Kiểm tra bàn phím vật lý: Kiểm tra xem có thiết bị nào gắn giữa bàn phím và máy tính không.

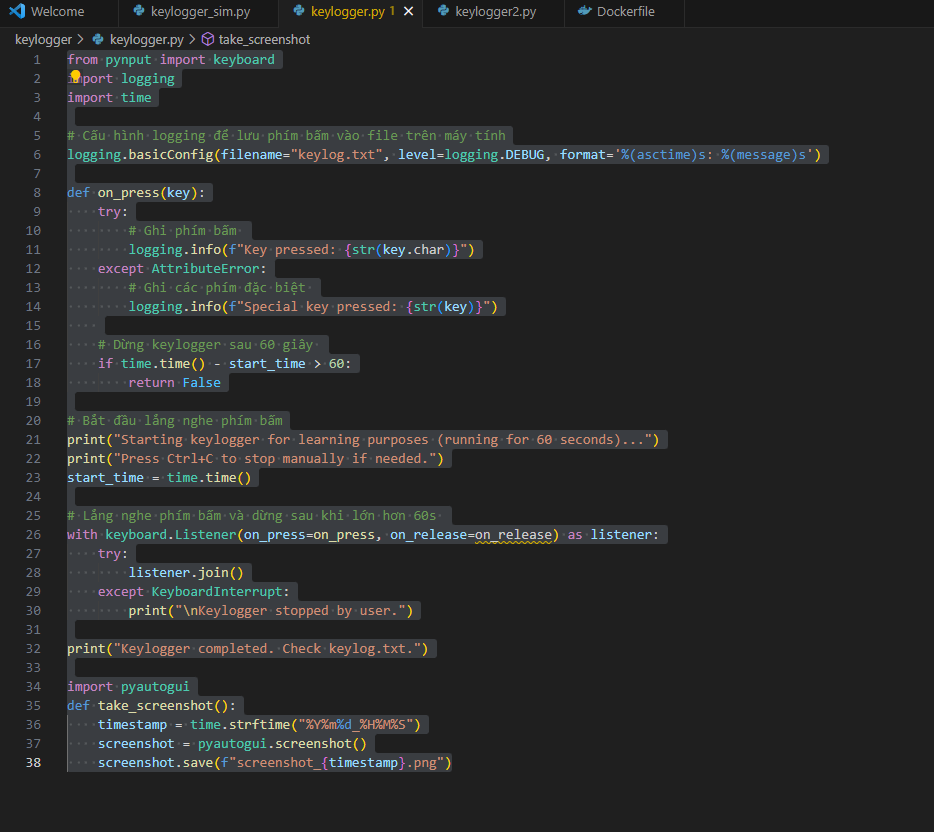
Sử dụng bàn phím không dây hoặc Bluetooth: Một số Hardware Keylogger chỉ hoạt động với bàn phím có dây.

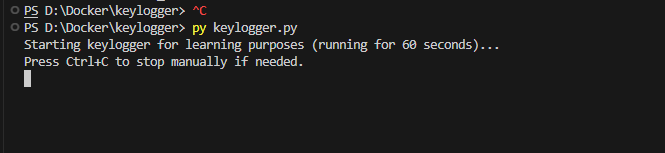
**Bài làm :**

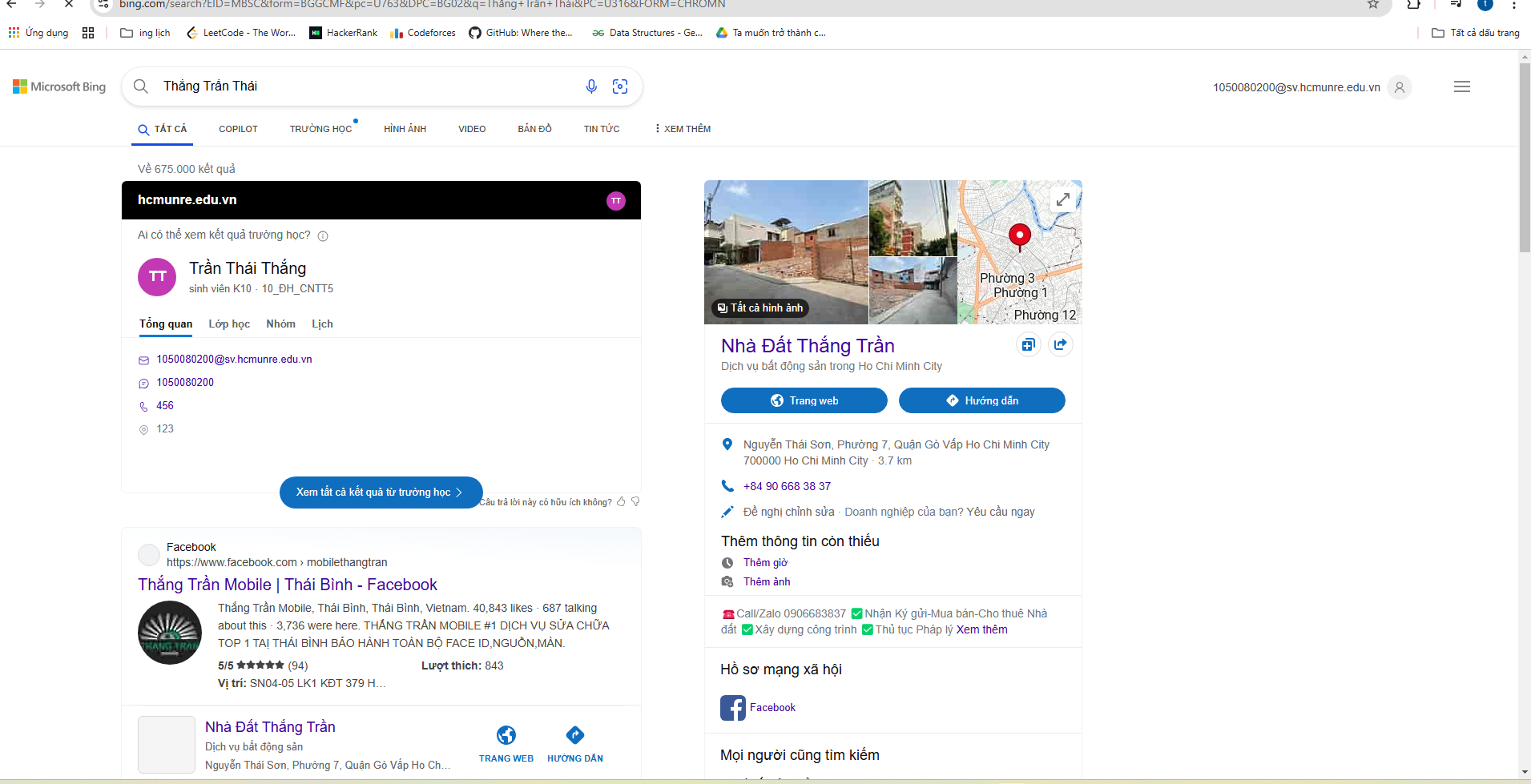
**1.Thử nghiệm Keylogger đơn giản :**

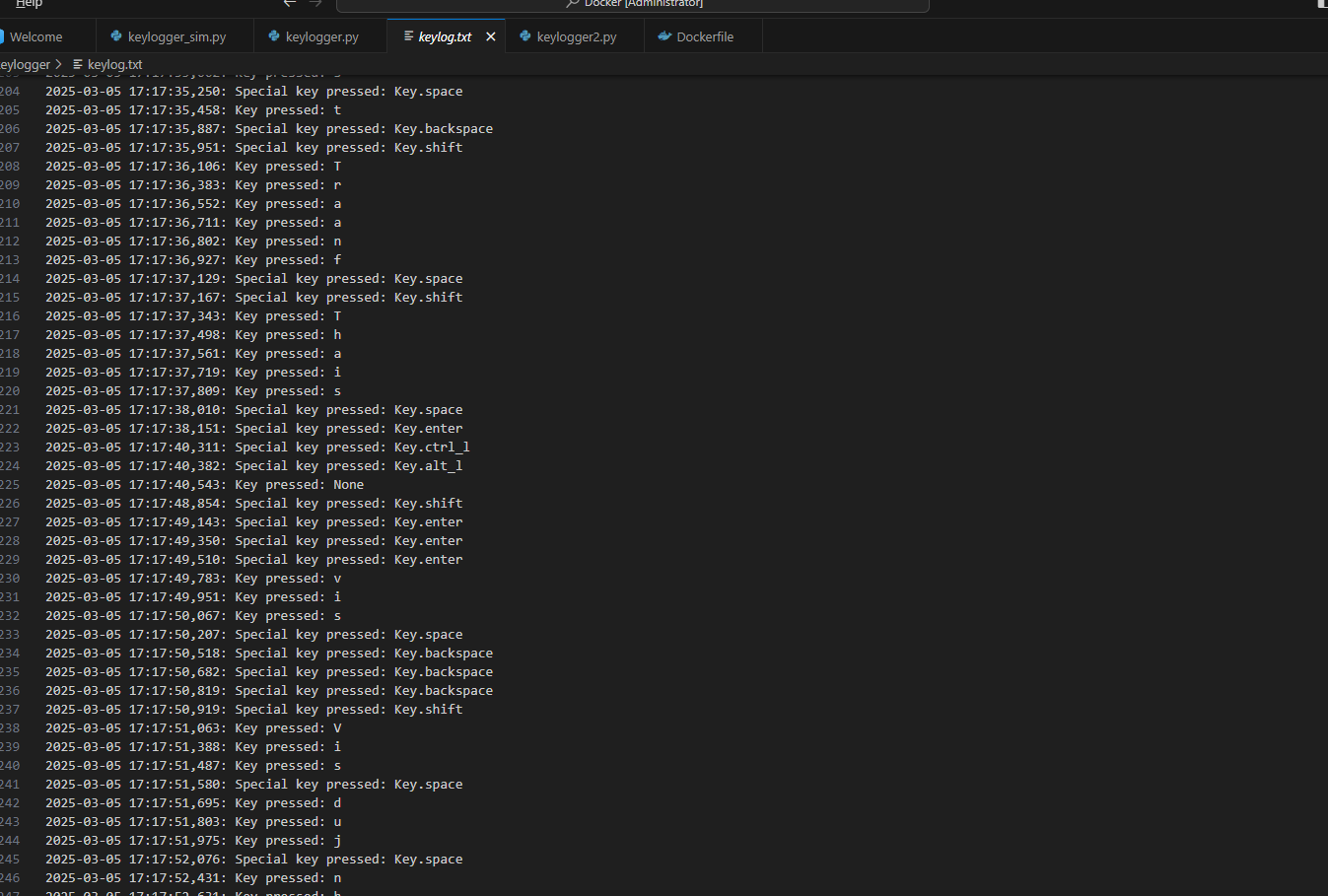
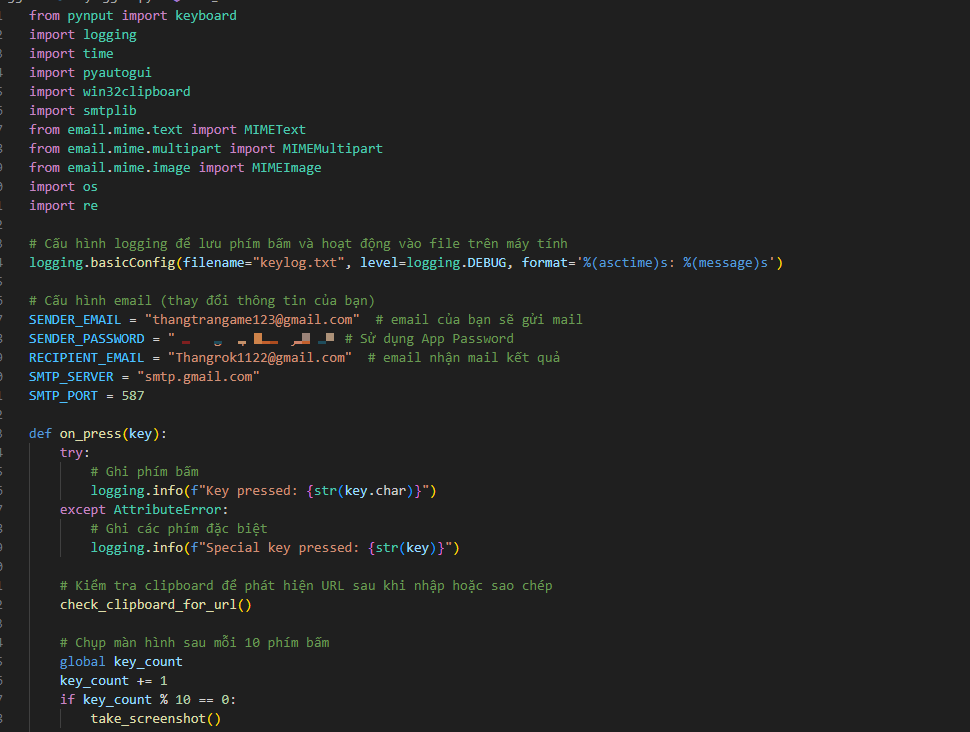
( Do e không cài máy ảo và docker cũng không có quyền truy cập vào tài nguyên vật lý của máy chủ nên việc cài đặt và sử dụng Keylogger ở docker là bất khả thi )

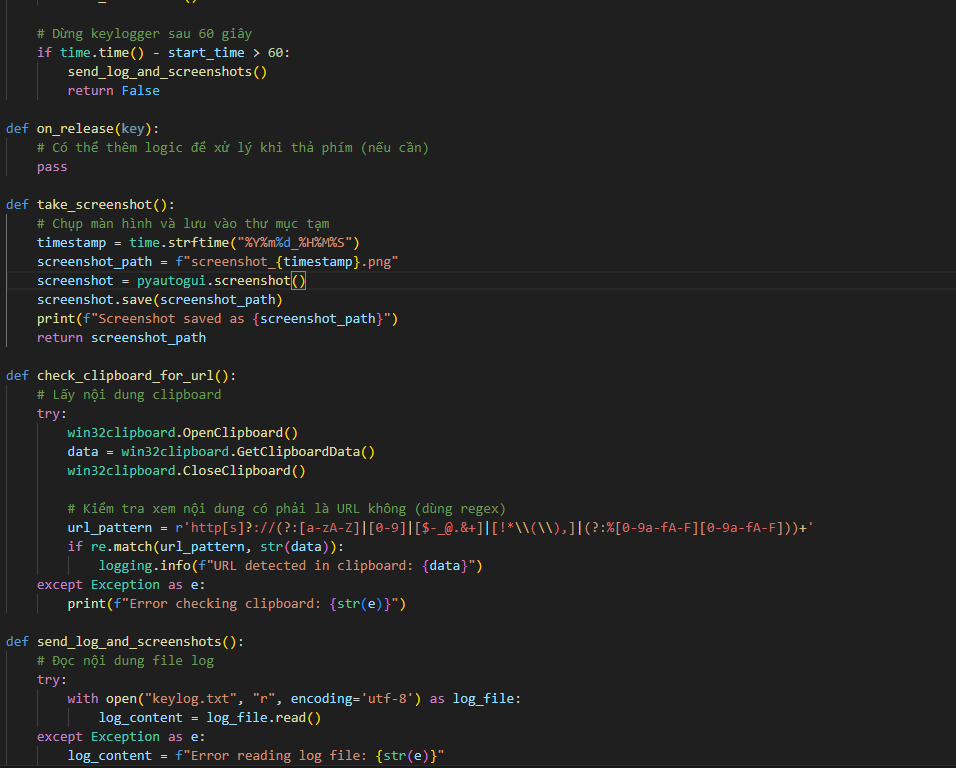
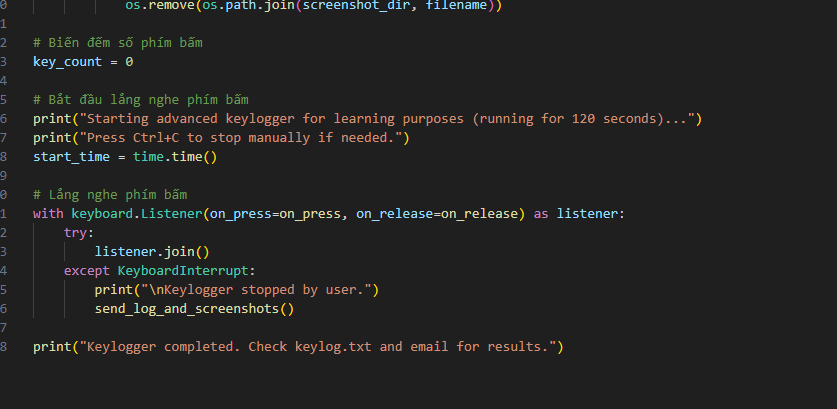
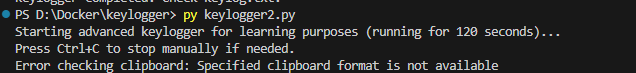
Sử dụng 1 mã code(độc) để nghiên cứu cách hoạt động của Keylogger :

  
  
lưu ý : Mã code không nên sử dụng ngoài mục đích học tập hoặc nghiên cứu   
  
Run mã

  
  
  
  
  
  
Ví dụ nhập

  
  
  
File trả về kết quả :

  
  
  
  
**2.Thử nghiệm Keylogger gửi về email và gửi cả hình ảnh**   
  
  
  
Mã độc   
  
  
  
  
vùng App password xin phép em được làm mờ

  
  
  
  
  
  
  
  
Done. Run file   
  
  
  
  
Kiểm tra email nhận file

