# **LỜI MỞ ĐẦU**

Theo xu hướng phát triển của xa hội ngày nay, ngành công nghệ thông tin là một trong những ngành không thể thiếu, dịch vụ internet ngày càng phát triển mở rộng trên toàn thế giới, việc truy cập internet ngày càng phổ biến. Mọi người ai cũng muốn internet nâng cao khả năng và hỗ trợ công việc cho bản thân mình.

Việc ứng dụng công nghệ thông tin vào kinh doanh, các trường học, cơ quan là một trong những yếu tố rất quan trọng để đưa nước ta sánh vai cùng các cường quốc năm châu. Đất nước ngày càng phát triển cùng với nhiều sự chuyển biến trên thế giới nên tin học với con người là xu thế tất yếu để hội nhập với nền công nghiệp mới. Để đảm bảo cho việc truy cập internet một cách an toàn và tránh khỏi sự dòm khó của những kẻ xấu muốn lợi dụng internet với những mục đích không tốt.

Em quyết định chọn đề tài: **“Tìm hiểu về Keylogger và Xây dựng ứng dụng”** dưới sự hướng dẫn của Thầy **Tiến sĩ Lê Đắc Nhường**. Đề tài này rất thực tế, phù hợp với tình hình hiện nay. Giúp em có thêm kinh nghiệm về bảo mật và an ninh mạng và dễ dàng thích nghi vào công việc sau khi ra trường.

Mục đích của đề tài này là tìm hiểu về Keylogger và Xây dựng ứng trụng để đánh cắp thông tin dữ liệu từ máy nạn nhân.

UBND THÀNH PHỐ HẢI PHÒNG **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**TRƯỜNG ĐẠI HỌC HẢI PHÒNG** **Độc lập – Tự do – Hạnh phúc**

**PHIẾU NHẬN XÉT CỦA CÁN BỘ HƯỚNG DẪN**

**ĐỒ ÁN, KHOÁ LUẬN TỐT NGHIỆP**

Họ và tên sinh viên: Nguyễn Văn Đông Lớp: ĐH.CNTT.2.K19

Ngày sinh: 04/07/2000 Nơi sinh: Hải Phòng

Tên đề tài: Tìm hiểu cơ chế hoạt động của Keylogger và Xây dựng ứng dụng

Giảng viên hướng dẫn : TS. Lê Đắc Nhường

*1.Ý thức tổ chức, kỷ luật trong quá trình nghiên cứu*

*......................................................................................................................................................*

*......................................................................................................................................................*

*......................................................................................................................................................*

*......................................................................................................................................................*

*2. Khả năng nghiên cứu và vận dụng kiến thức:*

*......................................................................................................................................................*

*......................................................................................................................................................*

*......................................................................................................................................................*

*......................................................................................................................................................*

*......................................................................................................................................................*

*3. Các nhận xét khác* *(nếu có)*......................................................................................................

......................................................................................................................................................

......................................................................................................................................................

........................................................................................................................................... .........

......................................................................................................................................................

**CÁN BỘ HƯỚNG DẪN**

*(Ký, ghi rõ họ tên))*

UBND THÀNH PHỐ HẢI PHÒNG **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**TRƯỜNG ĐẠI HỌC HẢI PHÒNG** **Độc lập – Tự do – Hạnh phúc**

**PHIẾU NHẬN XÉT CỦA CÁN BỘ PHẢN BIỆN**

**ĐỒ ÁN, KHOÁ LUẬN TỐT NGHIỆP**

Tên đề tài: Tìm hiểu cơ chế hoạt động của Keylogger và Xây dựng ứng dụng

Sinh viên thực hiện: Nguyễn Văn Đông Ngày sinh: 04/07/2000

Lớp: ĐH.CNTT.2.K19 Khóa: 2018-2022

Họ và tên cán bộ phản biện:.................................................................................................

Cơ quan công tác:................................................................................................................

**I.Nội dung của bản phản biện:**

1. Tính cần thiết, thời sự, ý nghĩa khoa học và thực tiễn của đề tài đồ án, khóa luận.

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

2. Kết cấu hình thức và nội dung trình bày của đồ án, khóa luận.

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

**II. Kết luận**

1.Nhận xét chung về kết quả nghiên cứu.

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

2.Đánh giá, chấm điểm *(theo thang điểm 10).*

Điểm số:……………….................................................................................

Điểm chữ:………………...............................................................................

*Hải Phòng, ngày…..tháng …năm 2020*

Cán bộ phản biện

(Ký và ghi rõ họ và tên)

# **LỜI CẢM ƠN**

Trước hết em xin gửi lời cảm ơn và lòng biết ơn đến Thầy **Tiến sĩ Lê Đắc Nhường** Giảng viên Trường Đại học Hải Phòng đã tận tình hướng dẫn trong suốt thời gian thực hiện chuyên đề. Thầy đã tạo rất nhiều điều kiện thuận lợi và cho những lời khuyên quý báu giúp em hoàn thành tốt chuyên đề.

Xin chân thành cảm ơn thầy cô giáo trong Trường Đại học Hải Phòng nói chung, các thầy cô trong Bộ môn Công Nghệ Thông Tin nói riêng đã tận tình giảng dạy, truyền đạt cho em những kiến thức quý báu và tạo điều kiện giúp đỡ trong suốt quá trình học tập trong những năm học vừa qua, giúp em có được cơ sở lý thuyết vững vàng.

Cuối cùng, em xin chân thành cảm ơn gia đình và bạn bè, đã luôn tạo điều kiện, quan tâm, ủng hộ, giúp đỡ, động viên em trong suốt quá trình học tập và hoàn thành chuyên đề.

Em xin chân thành cảm ơn!

Người thực hiện đề tài

**Nguyễn Văn Đông**

# **MỤC LỤC**

**LỜI MỞ ĐẦU** 1

**LỜI CẢM ƠN** 5

**MỤC LỤC** 6

**TÓM TẮT** 7

**CHƯƠNG 1. TÌM HIỂU VỀ KEYLOGGER** 8

1.1. Lịch sử về Keylogger 8

1.2. Khái niệm về Keylogger 8

1.3. Phân loại Keylogger 8

1.4. Cách hoạt động của Keylogger 9

1.5. Phòng, tránh và chống keylogger 10

**CHƯƠNG 2. XÂY DỰNG ỨNG DỤNG** 14

2.1. Các thư viện cần thiết 14

2.2. Các hàm cần thiết 14

2.3. Source Code 14

**CHƯƠNG 3. KẾT QUẢ NHẬN XÉT ĐÁNH GIÁ** 15

**CHƯƠNG 4. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN** 17

**TÀI LIỆU THAM KHẢO** 18

# **TÓM TẮT**

Chắc hẳn trong chúng ta, nhiều người đã không dưới 1 lần nghe tới khái niệm “keylogger”. Tuy chỉ có thể cảm nhận mơ hồ rằng đó là thứ nguy hiểm, một công cụ lợi hại có thể giúp kẻ xấu lấy cắp thông tin mà ta nhập vào từ bàn phím. Nhưng liệu bạn đã có thể tự tin nói rằng mình hoàn toàn hiểu đúng về thứ công cụ này?

Hãy cùng chúng tôi tìm hiểu về keylogger, mục đích sử dụng của nó, loại thông tin nó thu thập cũng như cách thức nó hoạt động, từ đó rút ra những kinh nghiệm bảo vệ bản thân một cách hiệu quả nhất.

# **CHƯƠNG 1. TÌM HIỂU VỀ KEYLOGGER**

## Lịch sử về Keylogger

Keylogger đã tồn tại trong rất nhiều năm qua. Lịch sử của Keylogger không thể biết chính xác. Người ta tin rằng nó được xuất hiện đầu tiên bởi chính phủ và không biết ngày phát hành chính xác của Keylogger. Tuy nhiên cũng có nhiều người tin rằng nó được xuất hiện trong đầu những năm 90.

## Khái niệm về Keylogger

Keylogger hay "trình theo dõi thao tác bàn phím" theo cách dịch ra tiếng Việt là một chương trình máy tính ban đầu được viết nhằm mục đích theo dõi và ghi lại mọi thao tác thực hiện trên bàn phím vào một tập tin nhật ký (log) để cho người cài đặt nó sử dụng. Vì chức năng mang tính vi phạm vào riêng tư của người khác này nên các trình keylogger được xếp vào nhóm các phần mềm gián điệp.

Về sau, khi keylogger phát triển cao hơn nó không những ghi lại thao tác bàn phím mà còn ghi lại cả các hình ảnh hiển thị trên màn hình (screen) bằng cách chụp (screen-shot) hoặc quay phim (screen-capture) thậm chí còn ghi nhận cách con trỏ chuột trên máy tính di chuyển.

## Phân loại Keylogger

Keylogger bao gồm hai loại, một loại keylogger phần cứng và một loại là phần mềm.

Theo những người lập trình, keylogger viết ra với chỉ có một loại duy nhất là giúp các bạn giám sát con cái, người thân xem họ làm gì với PC, với internet, khi chat với người lạ. Nhưng cách sử dụng và chức năng của keylogger hiện tại trên thế giới khiến người ta thường hay phân loại keylogger theo mức độ nguy hiểm bằng các câu hỏi:

* Nhiễm vào máy không qua cài đặt/Cài đặt vào máy cực nhanh (quick install)?
* Có thuộc tính ẩn/giấu trên trình quản lý tiến trình (process manager) và trình cài đặt và gỡ bỏ chương trình (Add or Remove Program)?
* Theo dõi không thông báo/PC bị nhiễm khó tự phát hiện?
* Có thêm chức năng Capturescreen hoặc ghi lại thao tác chuột?
* Khó tháo gỡ?
* Có khả năng lây nhiễm, chống tắt (kill process)?

Cứ mỗi câu trả lời "có", cho một điểm. Điểm càng cao, keylogger càng vượt khỏi mục đích giám sát (monitoring) đến với mục đích do thám (spying) và tính nguy hiểm nó càng cao. Keylogger có thể được phân loại theo số điểm:

### Loại số 1

* Không điểm: keylogger loại bình thường; chạy công khai, có thông báo cho người bị theo dõi, đúng với mục đích giám sát.

### Loại số 2

* Một đến hai điểm: keylogger nguy hiểm; chạy ngầm, hướng đến mục đích do thám nhiều hơn là giám sát (nguy hại đến các thông tin cá nhân như là tài khoản cá nhân, mật khẩu, thẻ tín dụng vì người dùng không biết).

### Loại số 3

* Ba đến năm điểm: keylogger loại rất nguy hiểm; ẩn giấu hoàn toàn theo dõi trên một phạm vi rộng, mục đích do thám rõ ràng.

### Loại số 4

* Sáu điểm: keylogger nguy hiểm nghiêm trọng, thường được mang theo bởi các trojan-virus cực kỳ khó tháo gỡ, là loại keylogger nguy hiểm nhất. Chính vì vậy (và cũng do đồng thời là "đồng bọn" của trojan-virus) nó thường hay bị các chương trình chống virus tìm thấy và tiêu diệt.

## 1.4. Cách hoạt động của Keylogger

### 1.4.1. Thành phần của Keylogger

Thông thường, một chương trình keylogger sẽ gồm có ba phần chính:

* Chương trình điều khiển (Control Program): dùng để theo điều phối hoạt động, tinh chỉnh các thiết lập, xem các tập tin nhật ký cho Keylogger. Phần này là phần được giấu kỹ nhất của keylogger, thông thường chỉ có thể gọi ra bằng một tổ hợp phím tắt đặc biệt.
* Tập tin hook, hoặc là một chương trình monitor dùng để ghi nhận lại các thao tác bàn phím, capture screen (đây là phần quan trọng nhất)
* Tập tin nhật ký (log), nơi chứa đựng/ghi lại toàn bộ những gì hook ghi nhận được.

Ngoài ra, tùy theo loại có thể có thêm phần chương trình bảo vệ (guard, protect), chương trình thông báo (report)…

### 1.4.2. Cách thức cài đặt vào máy

Các loại keylogger từ 1 - 3 thông thường khi cài đặt vào máy cũng giống như mọi chương trình máy tính khác, đều phải qua bước cài đặt. Đầu tiên nó sẽ cài đặt các tập tin dùng để hoạt động vào một thư mục đặc biệt (rất phức tạp), sau đó đăng ký cách thức hoạt động rồi đợi người dùng thiết lập thêm các ứng dụng. Sau đó nó bắt đầu hoạt động.

Loại keylogger số 4 có thể vào thẳng máy của người dùng bỏ qua bước cài đặt, dùng tính năng autorun để cùng chạy với hệ thống. Một số loại tự thả (drop) mình vào các chương trình khác, để khi người dùng sử dụng các chương trình này keylogger sẽ tự động chạy theo.

### 1.4.3. Cách hoạt động

Trong một hệ thống (Windows, Linux, Mac…), khi bấm 1 phím trên bàn phím, bàn phím sẽ chuyển nó thành tín hiệu chuyển vào CPU. CPU sẽ chuyển nó tới hệ điều hành để hệ điều hành dịch thành chữ hoặc số cho chính nó hoặc các chương trình khác sử dụng.

Nhưng khi trong hệ thống đó có keylogger, không những chỉ có hệ điều hành theo dõi mà cả hook file/monitor program của keylogger theo dõi nó sẽ ghi nhận và dịch lại các tính hiệu ghi vào tập tin nhật ký. Đồng thời nó còn có thể theo dõi cả màn hình và thao tác chuột.

## 1.5. Phòng, tránh và chống keylogger

### 1.5.1. Phòng

Keylogger thường bị vào máy qua hai con đường chính: được cài đặt hoặc bị cài đặt.

**Phòng ngừa "được cài đặt"**

Phương pháp sau chỉ có tác dụng với chủ máy (người nắm quyền root/administrator) Cách tốt nhất là không cho ai sử dụng chung máy tính. Bảo mật máy bằng cách **khóa** lại bằng các chương trình bảo vệ, hoặc mật khẩu khi đi đâu đó. Nếu phải dùng chung nên thiết lập quyền của người dùng chung đó **thật thấp** (guest đối với Windows XP, user đối với Linux) để kiểm soát việc cài đặt chương trình của họ.

**Phòng ngừa "bị cài đặt"**

Bị cài đặt là cách để nói đến các trường hợp keylogger vào máy không do người nào đó trực tiếp đưa vào trên máy đó mà do trojan, virus, spyware cài đặt vào máy nạn nhân mà nạn nhân không hề hay biết. Các biện pháp phòng ngừa:

* Không tùy tiện mở các tập tin lạ, không rõ nguồn gốc. Tốt nhất là nên xóa đi, hoặc kiểm tra (scan) bằng một chương trình antivirus và một chương trình antispyware, vì nhiều chương trình antivirus chỉ có thể tìm thấy virus, không thể nhận biết spyware.
* Không vào các trang web lạ, đặc biệt là web "tươi mát" vì có thể các trang web này ẩn chứa một loại worm, virus, hoặc là mã độc nào đó có thể âm thầm cài đặt.
* Không click vào các đường link lạ do ai đó cho bạn.
* Không cài đặt các chương trình lạ (vì nó có thể chứa virus, trojan)
* Không download chương trình từ các nguồn không tin cậy. Nếu bạn có thể, xem xét chữ ký điện tử, để chắc chắn chương trình không bị sửa đổi.
* Hạn chế download và sử dụng cracked-program.
* Luôn luôn tự bảo vệ mình bằng các chương trình chuyên dùng chống virus, chống spyware (antivirus, antispyware) và dựng tường lửa (firewall) khi ở trong Internet.
* Thường xuyên cập nhật đầy đủ các bản cập nhật bảo mật của hệ điều hành.
* Hoặc chúng ta có thể download một số phần mềm chống keylog về để bảo vệ

### 1.5.2. Tránh keylogger

Khi nghi ngờ nó có keylogger mà không có điều kiện kiểm tra.

**Diệt tập tin hook, chương trình theo dõi**

Sử dụng một chương trình task manager (có thể gọi ra bằng tổ hợp phím tắt Ctrl+Alt+Del trên Windows) xem các chương trình đang chạy. Nếu bạn thấy process nào lạ (đặc biệt đối với Windows XP là các tập tin được chạy dưới User name không phải là System) chưa thấy bao giờ hãy tắt (end, kill) nó đi. Lưu ý, cách này có thể làm treo hệ thống nếu đó là một tập tin cần cho nó; vì vậy người dùng cần có kinh nghiệm.

**Che mắt keylogger**

Keylogger hoạt động trên nguyên tắc theo dõi bàn phím (monitoring keyboard) chỉ có rất ít có khả năng theo dõi chuột (dù có theo dõi được cũng không chính xác lắm) và có khả năng capture clipboard. Vì vậy dù hệ thống có keylogger (trừ các keylogger có khả năng quay phim) có thể được vượt qua bằng cách:

* Sử dụng **On-Screen Keyboard** (bàn phím trên màn hình) (trong windows gọi ra bằng Start/Run/osk) để nhập cách dữ liệu nhạy cảm (mật khẩu, thẻ tín dụng) bằng cách click chuột. Vì đây là cách nhập liệu nằm ngoài vùng theo dõi của các tập tin hook (vì không qua bàn phím) nên keylogger sẽ không ghi nhận được thông tin gì. Cách này dễ dùng nhưng người khác có thể trông thấy thông tin được nhập vào (tiếng lóng thường dùng là đá pass) từ đó bạn mất password.
* Sử dụng **Copy’n’Paste** (chép và dán): tìm một đoạn văn bản nào đó có các từ nằm trong đoạn thông tin muốn giấu (ví dụ: mật khẩu là password bạn hãy tìm một đoạn văn có các từ p, a, s, w, o, r, d (ví dụ to day Is a hot day, peter feel bad he want a cool drink or a ice-cream) copy từng chữ một và dán nó thành chữ password rồi gửi đi. Cách này có ưu điểm là dễ dùng nhưng khá rắc rối và kém hiệu quả nhất bởi vì nhiều keylogger có chức năng theo dõi clipboard.
* Sử dụng **type’n’Click** (bấm và nhấn): vì bản thân một keylogger thông thường không thể theo dõi các bấm chuột. Ví dụ muốn đánh một đoạn thông tin là password, đầu tiên hãy đánh một số từ có trong nó: psr rồi sử dụng chuột (không dùng bàn phím) chen ngang vào p và s đánh chữ a giữa s và r đánh chữ swo sau r là chữ d. Dòng thông tin nhập vào password nhưng trong tập tin nhật ký log keylogger ghi lại được là psraswod. Cách này khá hay nhưng không phù hợp với các thông tin dài vì dễ gây quên.

### 1.5.3. Chống keylogger

**Phương pháp đơn giản**

Nhanh hiệu quả nhất là diệt trừ toàn bộ các chương trình đang theo dõi bàn phím đi. Một số chương trình như là Keylogger Killer của Totto quét các process tìm các chương trình theo dõi cùng lúc quá nhiều ứng dụng (keylogger dùng cách này thường bằng một tập tin \*.dll) rồi đề nghị bạn tắt nó đi. Thế nhưng một số chương trình tốt (như các chương trình giúp gõ bàn phím Unikey, Vietkey) cũng dùng cách này nên có thể gây diệt lầm.

**Phương pháp nâng cao**

Sử dụng một chương trình chống spyware chuyên dùng. Các chương trình này sẽ tự động quét, phân tích các chương trình đang chạy cũng như trên máy để từ đó nhận biết các chương trình keylogger và tự động diệt. Một số chương trình còn có chế độ bảo vệ thời gian thực (Real-Time Protection) giúp bảo vệ bạn chống ngay khi spyware chuẩn bị cài vào máy.

Nhưng điểm gây khó khăn nhất của cách dùng này là đa số các chương trình sử dụng tốt đều phải trả tiền (ví dụ như Spyware Doctor của Pctools, McAfee Antispyware của McAfee, Bitdefender…)

Tuy thế vẫn có một số chương trình miễn phí và khá tốt như Ad-Aware SE, Spybot S&D, Spyblaster tuy rằng nó lâu lâu vẫn bắt hụt một số chương trình đặc biệt, nhưng nếu dùng kết hợp (cùng lúc cả hai hoặc cả ba) thi hiệu quả hầu như là hoàn toàn.(nói thêm: nếu bạn chạy 2-3 chương trình không phù hợp với nhau sẽ gây ra xung đột phần mềm chống virut)

Trong một số trường hợp, người dùng chọn cách chống Keylogger theo cách "sống chung với lũ". Lấy ví dụ về Keyscrambler là một trong số những phần mềm bảo vệ máy tính theo phương pháp này. Mọi dữ liệu về phím bấm được truyền đến Hệ điều hành và được Keyscrambler mã hóa trước (do keyscrambler tác động trực tiếp từ phần lõi Kennel), sau đó mới đến các phần mềm khác (bao gồm cả keylogger) và cuối cùng được giải mã lại cho đúng với các phím được gõ. Phương pháp này có thể vô hiệu hóa đa số các loại keylogger hiện tại, không yêu cầu người dùng cập nhật các trình anti-keylogger thường xuyên. Tuy nhiên, nó cũng có những điểm yếu riêng. Nếu keylogger được viết để ghi lại các phím sau khi chúng được giải mã (ví dụ: cài keylogger như là một addon của trình duyệt...) thì xem như đã vô hiệu hóa được keyscrambler, và nó cũng chỉ hỗ trợ một số phần mềm nhất định. Khi dùng chung với các phần mềm gõ tiếng Việt, người dùng sẽ phải tắt KeyScramble đi, đây là một sự phiền phức lớn dù nó minh chứng cho khả năng bảo mật của phần mềm này.

# **CHƯƠNG 2. XÂY DỰNG ỨNG DỤNG**

## 2.1. Các thư viện cần thiết

using System;

using System.Collections.Generic;

using System.Diagnostics;

using System.Drawing;

using System.Drawing.Imaging;

using System.IO;

using System.Linq;

using System.Net.Mail;

using System.Runtime.InteropServices;

using System.Text;

using System.Threading;

using System.Threading.Tasks;

using System.Windows.Forms;

using Microsoft.Win32;

## 2.2. Các hàm cần thiết

* HookKeyboard, SetHook, HookCallback: Các hàm bắt ký tự từ bàn phím
* WriteLog: Hàm ghi các ký tự bắt được vào file log
* HideWindow: Ẩn màn hình console
* DisplayWindow: Hiện màn hình console
* CheckHotKey: Sau khi chạy chương trình mặc định sẽ ẩn màn hình console để che mắt người dùng, ấn tổ hợp phím Ctrl + D sẽ ẩn/hiện màn hình console
* CaptureScreen: Hàm chụp màn hình
* SendMail: Hàm gửi file log và file chụp màn hình về mail
* StartTimmer: Cứ sau một khoảng thời gian thì tự chụp màn hình và gửi mail
* StartWithOS: Đăng ký khởi động cùng Windows

## 2.3. Source Code

<https://github.com/nguyendong47/ChuyenDeAnToanDuLieu/tree/master/ChuyenDe36/Keylogger%20Visual%20Studio>

# **CHƯƠNG 3. KẾT QUẢ NHẬN XÉT ĐÁNH GIÁ**

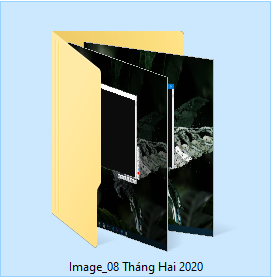
## 3.1. Đã bắt được phím khi nạn nhân ấn từ bàn phím

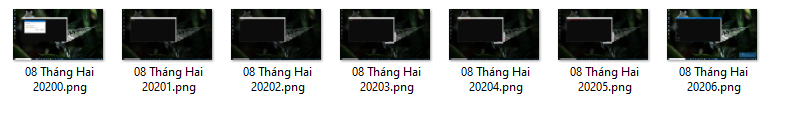
**Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo tự động**

## 3.2. Các phím bắt được đã được ghi vào file log.txt **Ảnh có chứa ảnh chụp màn hình Mô tả được tạo tự động**

## 3.3. Đã chụp được màn hình máy nạn nhân

****



## 3.4. Đã gửi kết quả về gmail thành công

**Ảnh có chứa ảnh chụp màn hình

Mô tả được tạo tự động**

# **CHƯƠNG 4. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

**Kết Luận :** Do giới hạn thời gian và em chưa có hiểu biết sâu về HĐH windows cùng một số thư viện cũng như các hàm cần thiết. Em đã viết được một chương trình Keylogger hiện tại mới ở mức độ đơn giản.

**Hướng Phát Triển :** Trong tương lai em sẽ cố gắng hoàn thiện thêm một số chức năng nữa cho Keylogger, để Keylogger này tuy chỉ dùng với mục đích giám sát nhưng sẽ hiệu quả và mang tính chất thực tiễn tốt hơn. Trong quá trình thực hiện, dù đã rất cố gắng, nhưng do trình độ, kiến thức, thời gian còn nhiều hạn chế, không thể tránh khỏi những thiếu sót. Em rất mong được sự đóng góp ý kiến, sửa chữa, và định hướng phát triển chuyên đề được hoàn thiện hơn. Rất cám ơn thầy cô đã dành thời gian để đọc và đánh giá chuyên đề.

# TÀI LIỆU THAM KHẢO

<https://vi.wikipedia.org/wiki/Keylogger>

<https://quantrimang.com/tim-hieu-ve-keylogger-va-cach-phong-tranh-108996>

<https://www.slideshare.net/vumanhson98/tm-hiu-keylogger-v-thit-k-chng-trnh-keylogger>