**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**TIỂU LUẬN CUỐI KÌ**

**CHUYÊN ĐỀ AN NINH MẠNG**

Đề tài:

**TÌM HIỂU LỖ HỔNG CVE-2017-8464**

Người hướng dẫn : TS. NGUYỄN HỒNG SƠN

Sinh viên thực hiện : Nguyễn Tuấn Kiệt

Mã số sinh viên : N18DCAT035

Lớp : D18CQAT01-N

Khóa : 2018 – 2023

Hệ : ĐẠI HỌC CHÍNH QUY

TP.HCM, tháng 11 năm 2022

# MỤC LỤC

[MỤC LỤC 2](#_Toc120140559)

[DANH MỤC CÁC TỪ VIẾT TẮT 3](#_Toc120140560)

[CHƯƠNG 1. TỔNG QUAN VỀ CVE-2017-8464 4](#_Toc120140561)

[1.1. KHÁI NIỆM VỀ FILE LNK 4](#_Toc120140562)

[1.2. TẠO HỆ THỐNG MẮC LỖI CVE-2017-8464 5](#_Toc120140563)

[1.3 CÔNG CỤ TẤN CÔNG LỖ HỔNG CVE-2017-8464 5](#_Toc120140564)

[CHƯƠNG 2: DEMO KHAI THÁC LỖ HỔNG SỬ DỤNG METASPLOIT 6](#_Toc120140565)

[2.1. GIỚI THIỆU METASPLOIT 6](#_Toc120140566)

[2.2. MÔ HÌNH KHAI THÁC 6](#_Toc120140567)

[2.3. TIẾN HÀNH KHAI THÁC 6](#_Toc120140568)

[CHƯƠNG 3: PHÂN TÍCH SIGNATURE CỦA CVE-2017-8464 DỰA TRÊN GÓI MẠNG BẮT ĐƯỢC 9](#_Toc120140569)

[3.1. PHÂN TÍCH SIGNATURE CỦA CVE-2017-8464 DỰA TRÊN GÓI MẠNG BẮT ĐƯỢC 9](#_Toc120140570)

[3.2. HÀM XỬ LÝ PHÁT HIỆN KHAI THÁC CVE-2017-8464 DỰA TRÊN PHÂN TÍCH SIGNATURE CỦA GÓI MẠNG 13](#_Toc120140571)

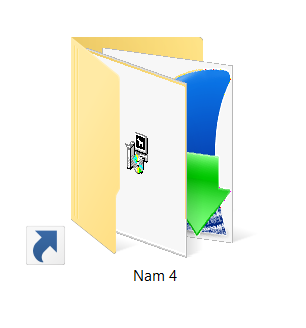
# DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| Từ viết tắt | Thuật ngữ tiếng Anh | Ý nghĩa |
| CVE | Common Vulnerabilities and Exposures | Danh sách các lỗ hổng bảo mật máy tính phổ biến |
| LNK | LINK | Các tệp LNK là các tệp lối tắt được liên kết với Windows và được phát triển bởi Microsoft Corporation. |
| DLL | Dynamic Link Library | File DLL chứa những hướng dẫn mà các chương trình khác có thể gọi đến để làm một tác vụ nào đó.  Về cơ bản, DLL cũng giống như EXEs, tuy nhiên các file này được đặt tên khác nhau trong quá trình liên kết. |

# CHƯƠNG 1. TỔNG QUAN VỀ CVE-2017-8464

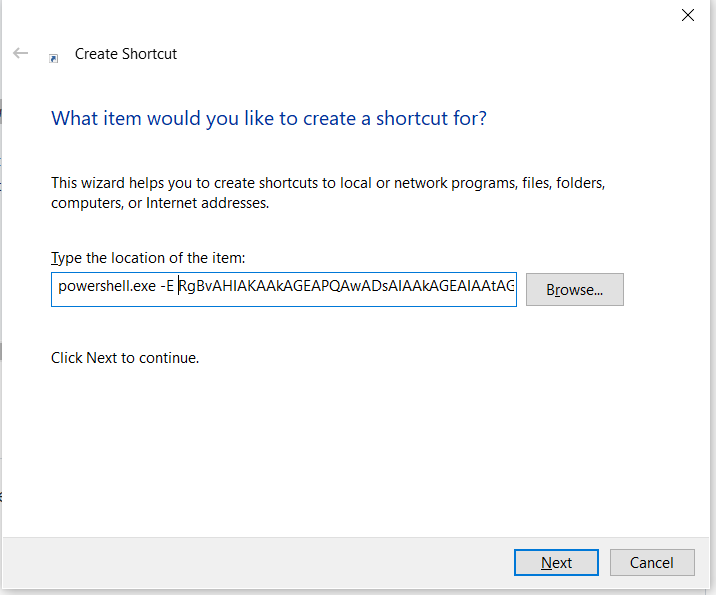
## 1.1. KHÁI NIỆM VỀ FILE LNK

LNK là System Files - Windows Shortcut, dưới định dạng Binary được phát triển bởi Microsoft.



Một tập tin LNK là một phím tắt hoặc "liên kết" được sử dụng bởi Windows như là một tham chiếu đến một gốc tập tin, thư mục, hoặc ứng dụng tương tự như một bí danh trên nền tảng Macintosh. Nó chứa các shortcut loại mục tiêu, vị trí và tên tập tin cũng như các chương trình mở các tập tin mục tiêu và một phím tắt tùy chọn. Các tập tin có thể được tạo ra trong Windows bằng cách kích chuột phải vào một tập tin, thư mục, hoặc chương trình thực thi và sau đó chọn Create shortcut.

Lợi dụng lỗ hổng này tồn tại trong Microsoft Windows cho phép kẻ tấn công thực hiện code từ xa nếu biểu tượng của một phím tắt hay shortcut (được tạo ra một cách đặc biệt).



Thành phần dễ bị tấn công được liên kết với network stack. Một lỗ hổng như vậy thường được gọi là “remotely exploitable” và có thể được coi là một cuộc tấn công có thể khai thác được ở protocol level hoặc nhiều network hops (ví dụ: qua một hoặc nhiều bộ định tuyến).

## 1.2. TẠO HỆ THỐNG MẮC LỖI CVE-2017-8464

Các hệ thống bị ảnh hưởng bới lỗ hổng CVE-2017-8464 là Windows Shell trong Microsoft Windows Server 2008 SP2 và R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold và R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703 và Windows Server 2016 cho phép người dùng cục bộ hoặc những kẻ tấn công từ xa thực thi mã tùy ý thông qua tệp .LNK được tạo thủ công, không được xử lý đúng cách trong khi hiển thị biểu tượng trong Windows Explorer hoặc bất kỳ ứng dụng nào khác phân tích cú pháp biểu tượng của lối tắt. Hay còn gọi là "LNK Remote Code Execution Vulnerability."

Bản cập nhật bảo mật vá lỗ hổng bằng cách sửa chữa xác nhận đúng tham chiếu của biểu tượng shortcut, Microsoft Windows đã có bản cập nhật cho lỗ hổng này vào tháng 6 năm 2017. Lỗ hổng này không ảnh hưởng đến phiên bản Windows XP và Windows cũ hơn.

## 1.3 CÔNG CỤ TẤN CÔNG LỖ HỔNG CVE-2017-8464

**Metasploit**

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service sử dụng trên giao diện dòng lệnh, công cụ này có sẵn trên kali linux phiên bản VMware.



# CHƯƠNG 2: DEMO KHAI THÁC LỖ HỔNG SỬ DỤNG METASPLOIT

## 2.1. GIỚI THIỆU METASPLOIT

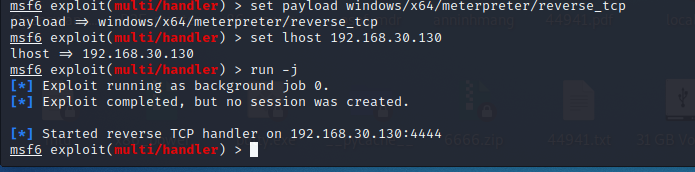
Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.

## 2.2. MÔ HÌNH KHAI THÁC

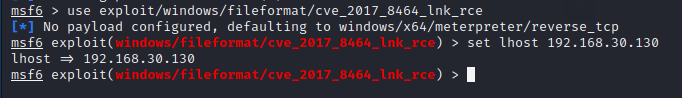
|  |  |  |
| --- | --- | --- |
| Attacker | Kali Linux | 192.168.30.130 |
| Victim | Windows 10 v1607 build 14393.0 | 192.168.30.150 |

## 2.3. TIẾN HÀNH KHAI THÁC

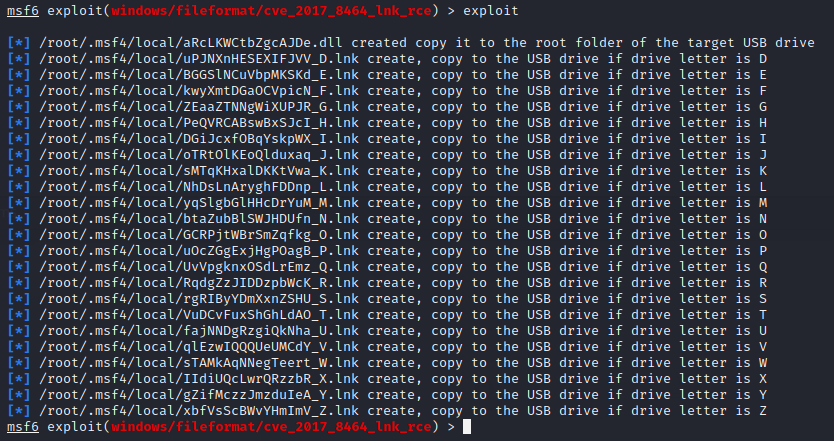
* Tạo payloads reverse\_tcp cho windows x64 và lắng nghe kết nối TCP đến máy Kali.
* Với LHOST là địa chỉ lắng nghe từ máy attacker.
* Với LPORT là port lắng nghe trên máy attacker.

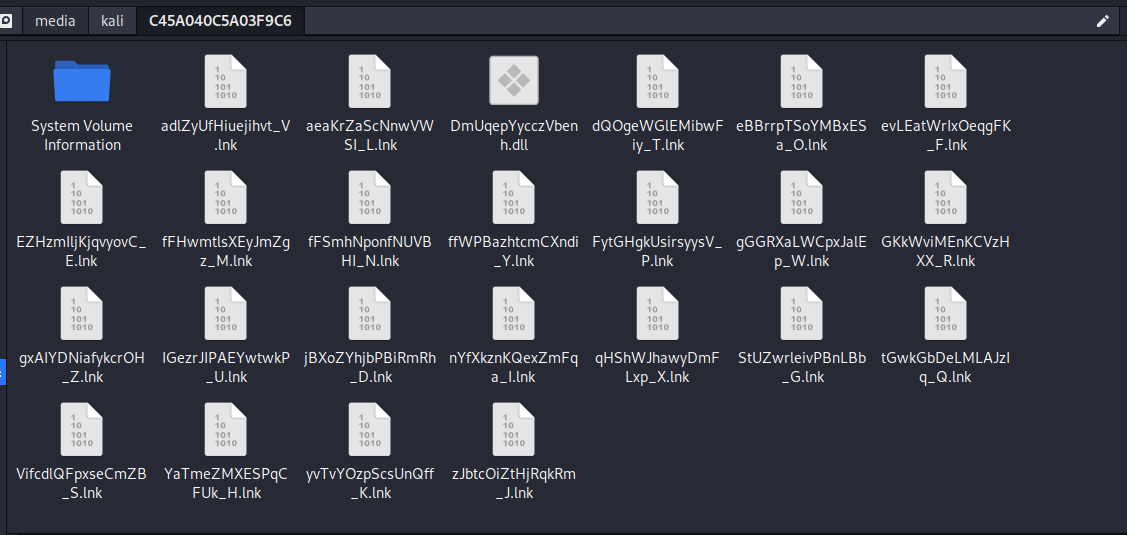


* Tạo file shortcut chứa lỗi CVE-2017-8464 để tự động khởi chạy payloads reverse\_tcp windows x64 được chèn vào.

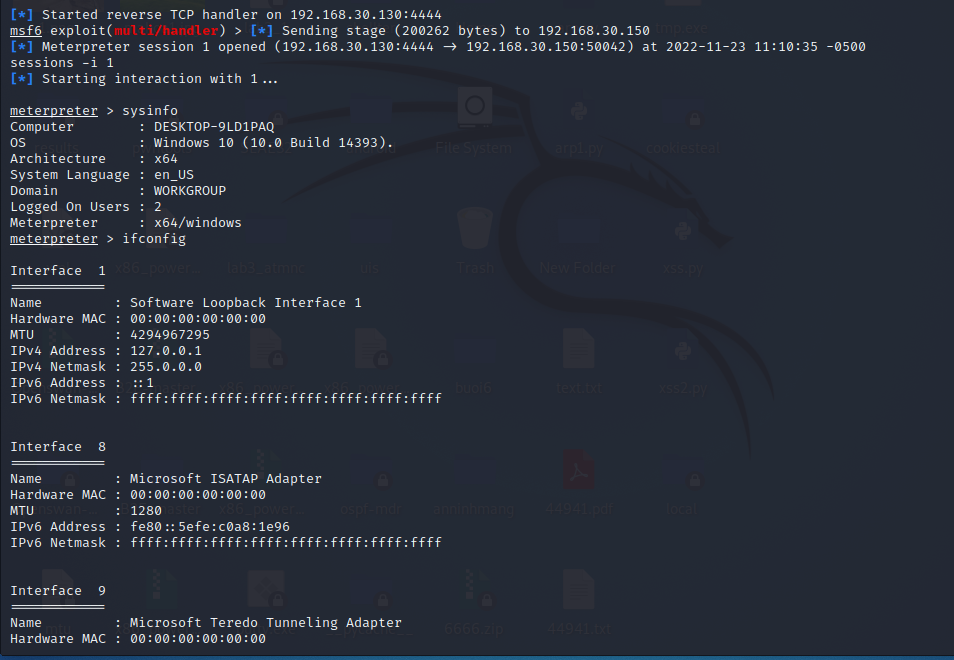


* Khởi chạy lênh exploit để khởi tạo các shortcut chứa lỗi trỏ tới file payload.
* Cụ thể như trong thông tin mô tả trên sẽ có file payload là FlashPlayerCPApp.cpl và file shortcut chứa lỗ hổng tự động chạy file payload.
* Sau khi khởi tạo hết các file cần thiết này nó sẽ lưu ra folder /root/.msf4/local/ trên máy kẻ tấn công rồi kẻ tấn công sẽ copy toàn bộ các file trong thư mục đó ra 1 USB bất kì.





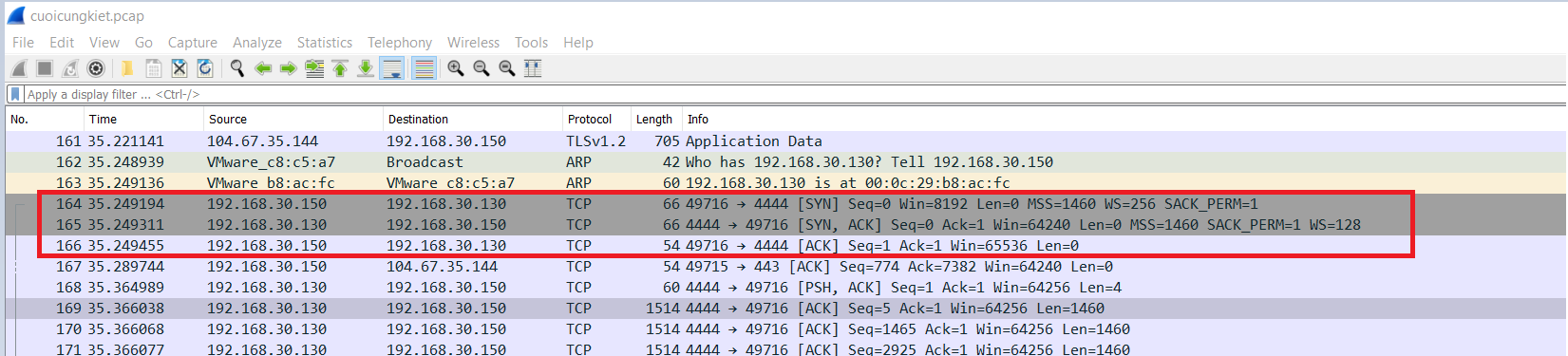
* Sau khi dụ dỗ nạn nhân cắm vào USB vào máy tính của họ. Nạn nhân không cần click bất cứ vào ứng dụng gì trong USB nhưng lỗi từ file .lnk (shortcut file) đã tự động khởi payload mã độc để thực hiện lỗ hổng chạy code thực thi từ xa.
* Quan sát lại trên máy attackers thì ta thấy máy nạn nhân đã kết nối đến máy kẻ tấn công lúc này kẻ tấn công đã khai thác thành công dựa trên CVE-2017-8464 và thực thi được mã độc từ xa đến máy nạn nhân.



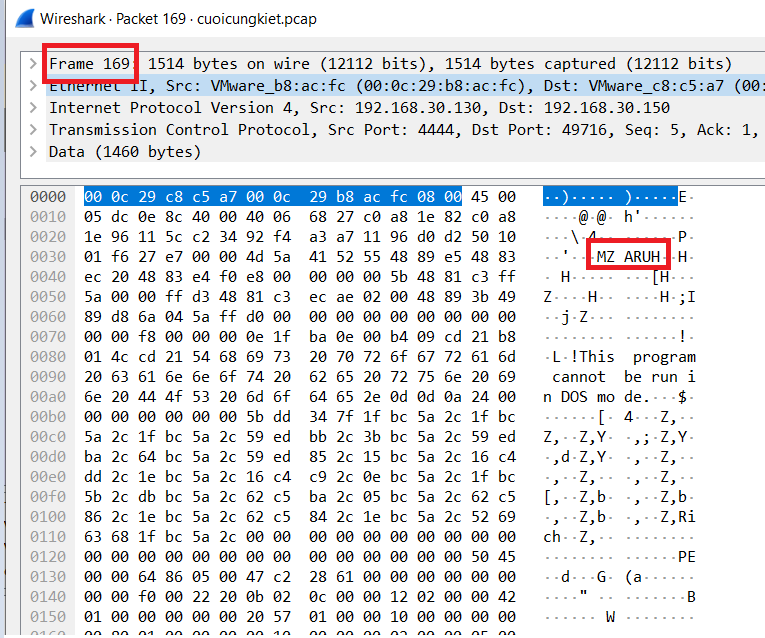
# CHƯƠNG 3: PHÂN TÍCH SIGNATURE CỦA CVE-2017-8464 DỰA TRÊN GÓI MẠNG BẮT ĐƯỢC

## 3.1. PHÂN TÍCH SIGNATURE CỦA CVE-2017-8464 DỰA TRÊN GÓI MẠNG BẮT ĐƯỢC

* Khi thực hiện cắm usb vào máy victimi bắt gói ta thấy rằng khi file .lnk tự động chạy thì máy nạn nhân gọi kết nối TCP đến địa chỉ máy kẻ tấn công đã thiết lập trong payloads.



* Tiếp theo gói tin với dấu hiệu đáng nghi “MZ” cho thấy đây có lẽ là 1 PE file mã độc để đưa về máy nạn nhân



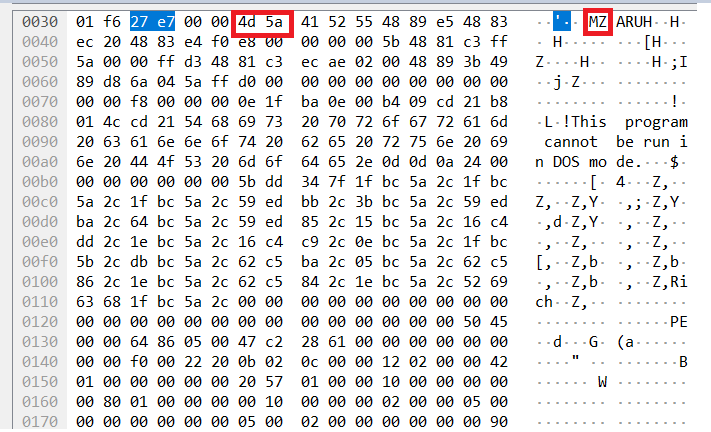
PE File Format (Portable Executable File Format): là định dạng file riêng của Win32. Tất cả các file có thể thực thi được trên Win32 như: \*.EXE, \*.DLL (32 bit),\*.COM,\*.NET, \*.CPL,… đều là định dạng PE; ngoại trừ các tập tin VxDs và \*.DLL (16 bit).

[](https://github.com/TrG-1999/DetectPacket-CVE-2017-8464/blob/main/018.png)

DOS MZ Header

Tất cả các PE file đếu bắt đầu bằng một DOS MZ Header đơn giản. Nó chiếm 64 bytes đầu tiên. Vùng này được dùng  trong trường hợp chương trình chạy trên nền DOS

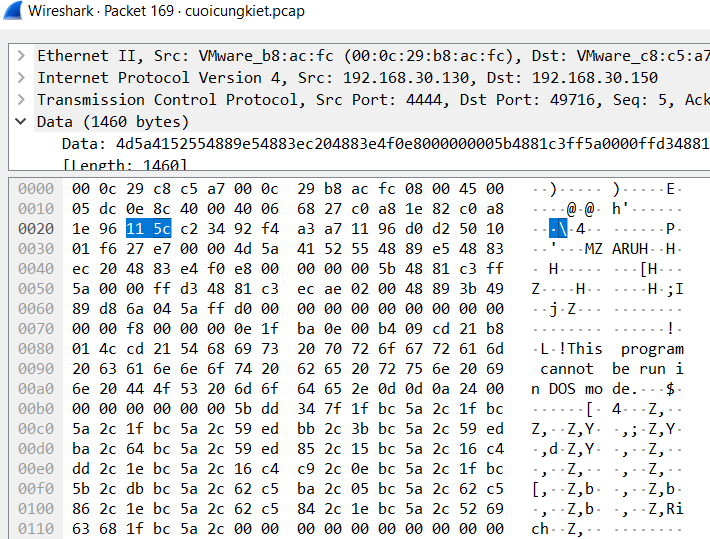
**e\_magic:** Chữ ký của PE file, giá trị: 4Dh, 5Ah (Ký tự “MZ”, tên của người sáng lập MS-DOS: Mark Zbikowsky). Giá trị này đánh dấu một DOS Header hợp lệ và được phép thực thi tiếp.



**e\_lfanew:** là một DWORD nằm ở cuối cùng của DOS Header, là trường chứa offset của PE Header so với vị trí đầu file.

DOS STUB

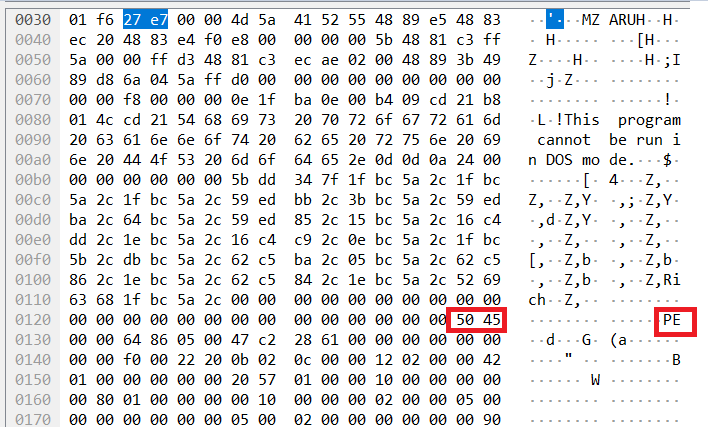
DOS Stub chỉ là một chương trình DOS EXE nhỏ hiển thị một thông báo lỗi, là phần để tương thích với Windows 16bit.



PE Header

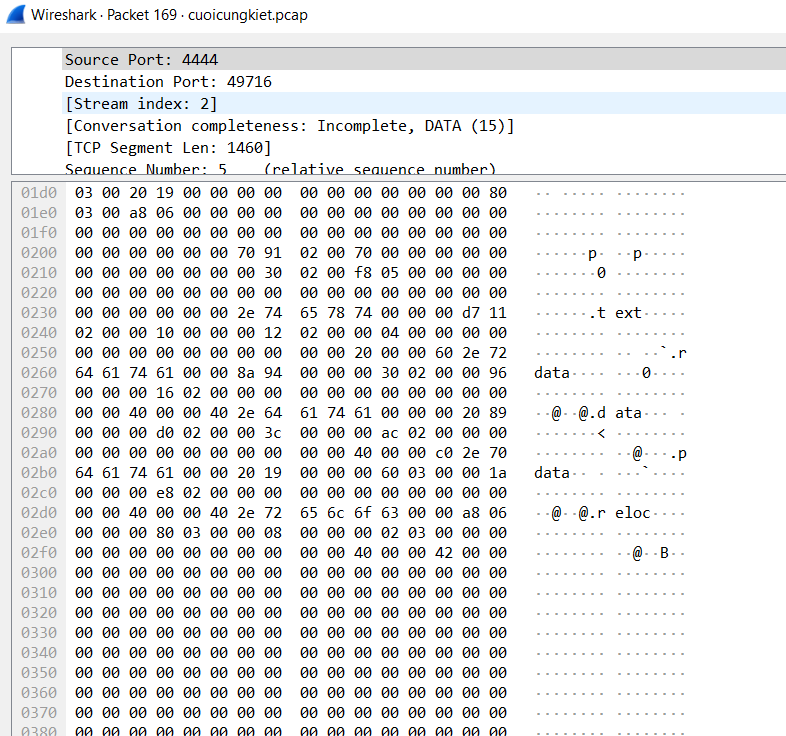
PE Header thực chất là cấu trúc IMAGE\_NT\_HEADERS bao gồm các thông tin cần thiết cho quá trình loader load file lên bộ nhớ.

**Signature:** là 1 DWORD bắt đầu PE Header chứa chữ ký PE: 50h, 45h, 00h, 00

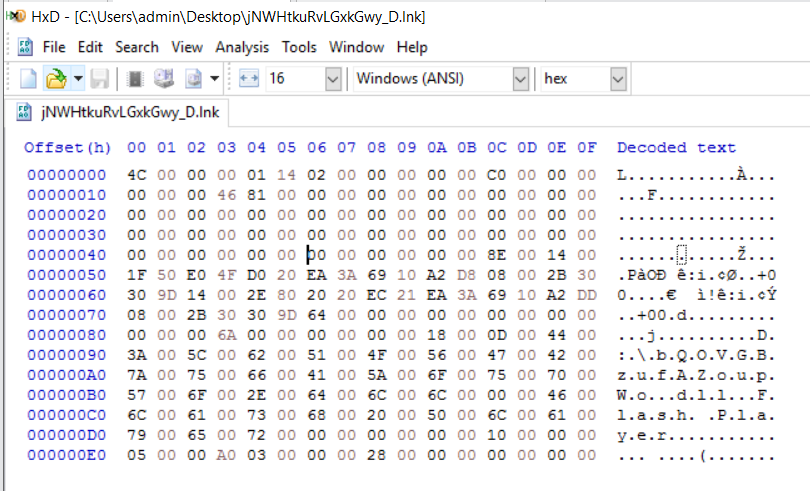


SECTION TABLE

Section Table là thành phần ngày sau PE Header, bao gồm một mảng những cấu trúc IMAGE\_SECTION\_HEADER

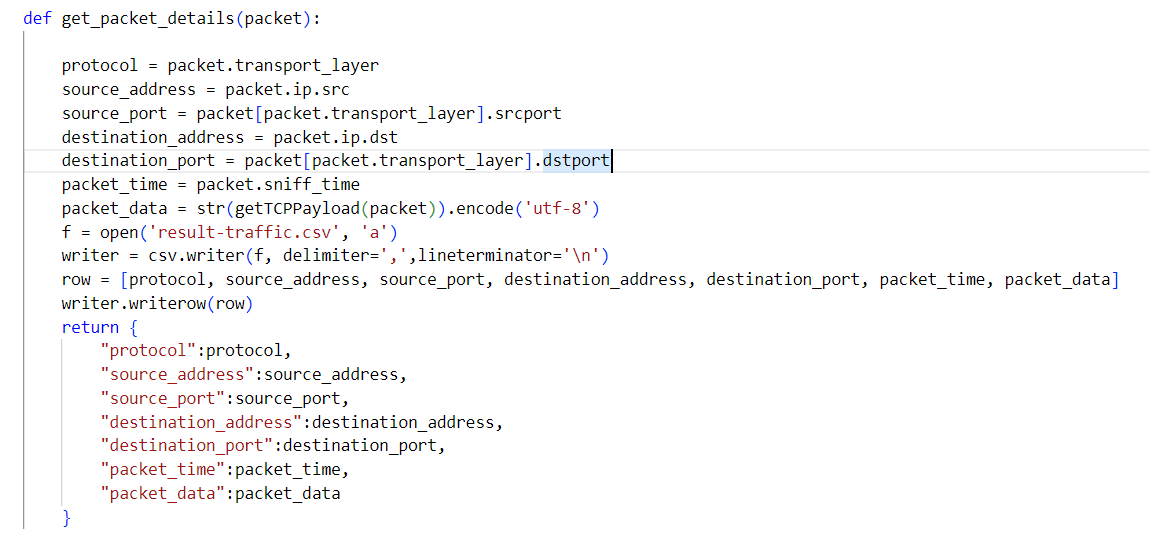


* Những gói tin tiếp theo sẽ là những phần dữ liệu của SECTION của PE file.
* Từ đó ta chỉ lấy phần HEADER trong cấu trúc của PE file mã độc này đem băm trên hàm MD5 để làm signature phát hiện ra mã độc của file này, cụ thể ta sẽ lấy 1024 bytes dữ liệu trong gói tin mà ta phát hiện, nó có bao gồm phần HEADER. Và những thông tin liên quan ta biết đễn mã độc sẽ được lưu trong file CSV để làm tập dữ liệu phát hiện các mã độc.
* Khi sử dụng Hex Editor mở file .lnk
* Thấy dc trong file lnk có gọi tới file dll nằm trong thư mục D:\bQOVGBzufAZoupWo.dllFlash Player
* Có 24 file LNK cho các ổ đĩa từ D-Z để khi usb được cắm vào máy thì file lnk sẽ gọi file DLL

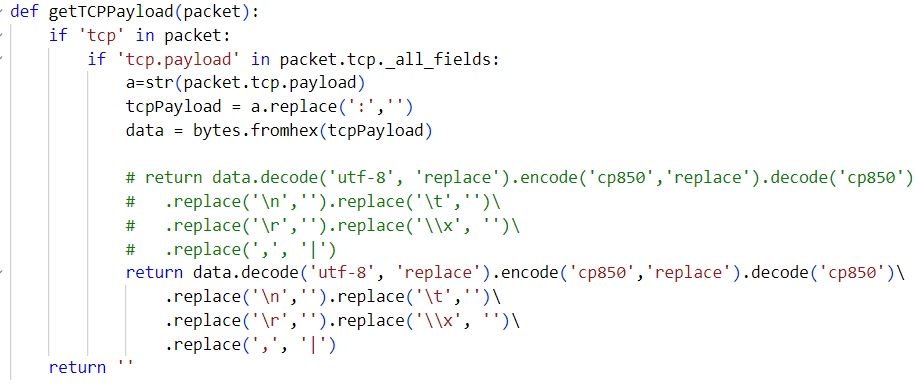


## 3.2. HÀM XỬ LÝ PHÁT HIỆN KHAI THÁC CVE-2017-8464 DỰA TRÊN PHÂN TÍCH SIGNATURE CỦA GÓI MẠNG

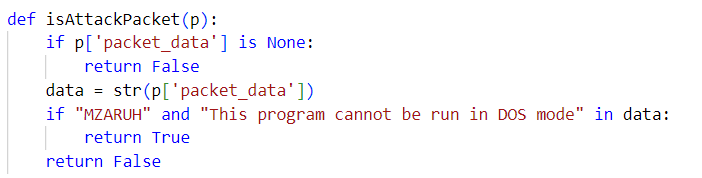
* Hàm **get\_packet\_details** sẽ lấy thông tin của packet.



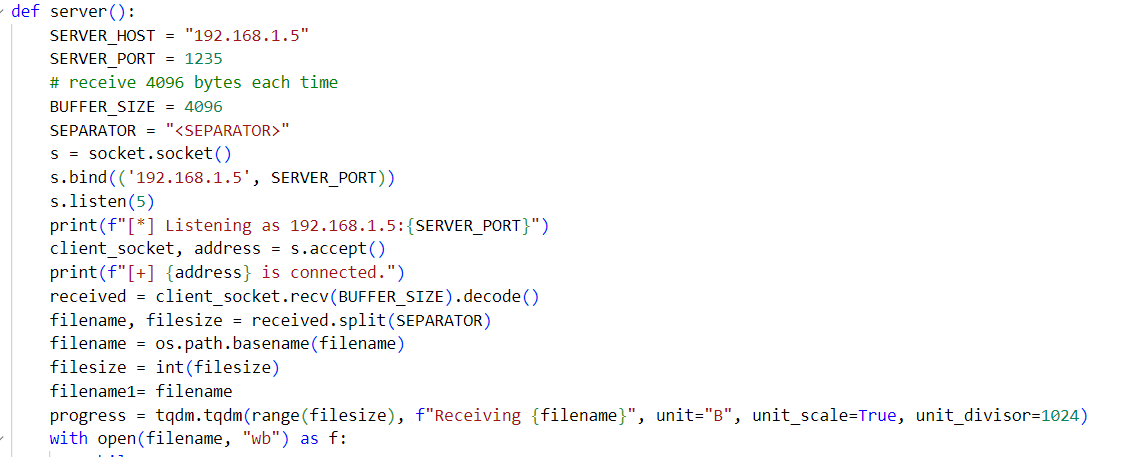
* Hàm **getTCPPayload** sẽ lấy data dạng hex trong gói tin và chuyển hex sang acsii

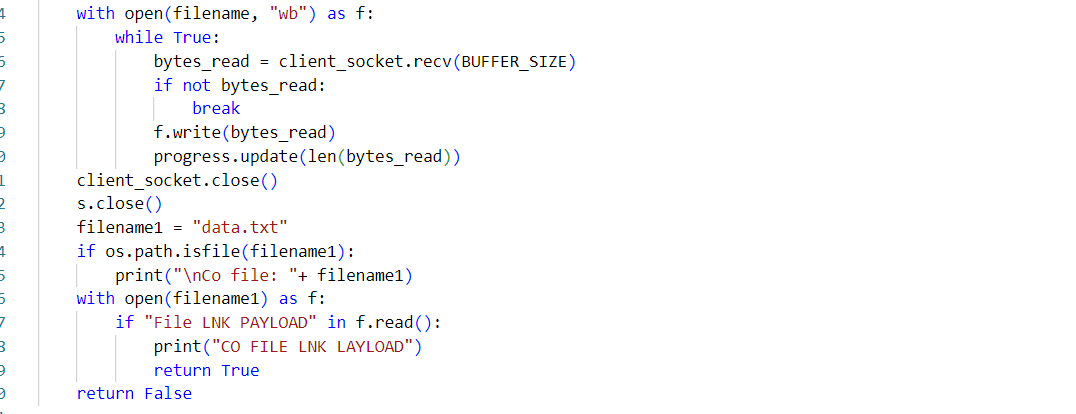


* Hàm **isAttackPacket** là hàm sẽ so sánh dữ liệu đã bắt được với signture reverse tcp

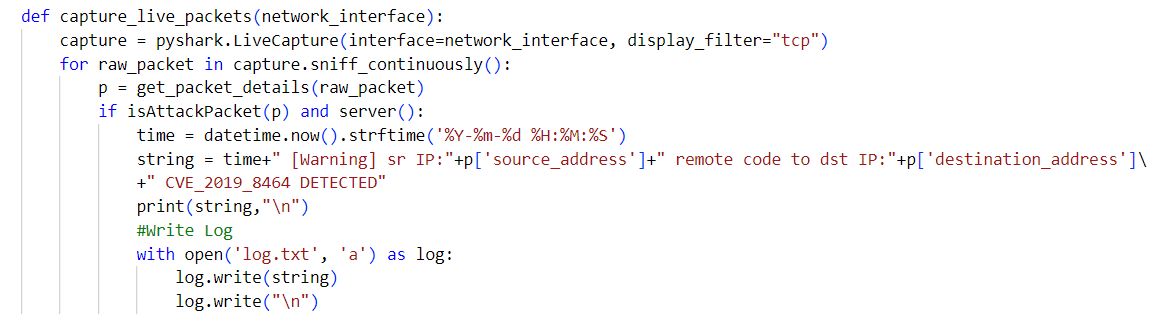


* Hàm **server** là hàm nhận dữ liệu usb đã scan từ máy client để phát hiện file lnk lỗi

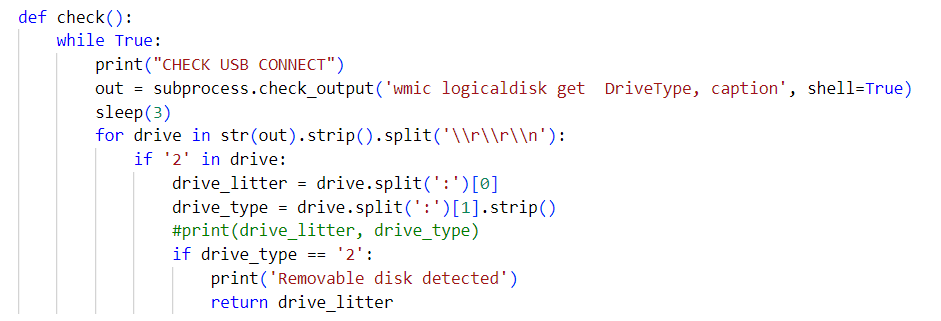




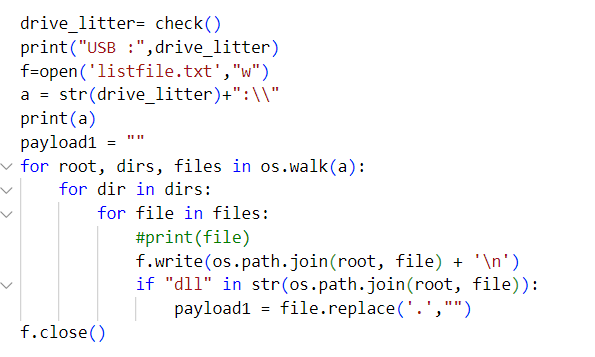
* Hàm **capture\_live\_packets** sẽ là hàm bắt gói tin và phát hiện tấn công dựng vào kết quả trả về của hàm isAttackPacket và hàm server để kết luận xem máy victim có bị tấn công CVE-2017-8464



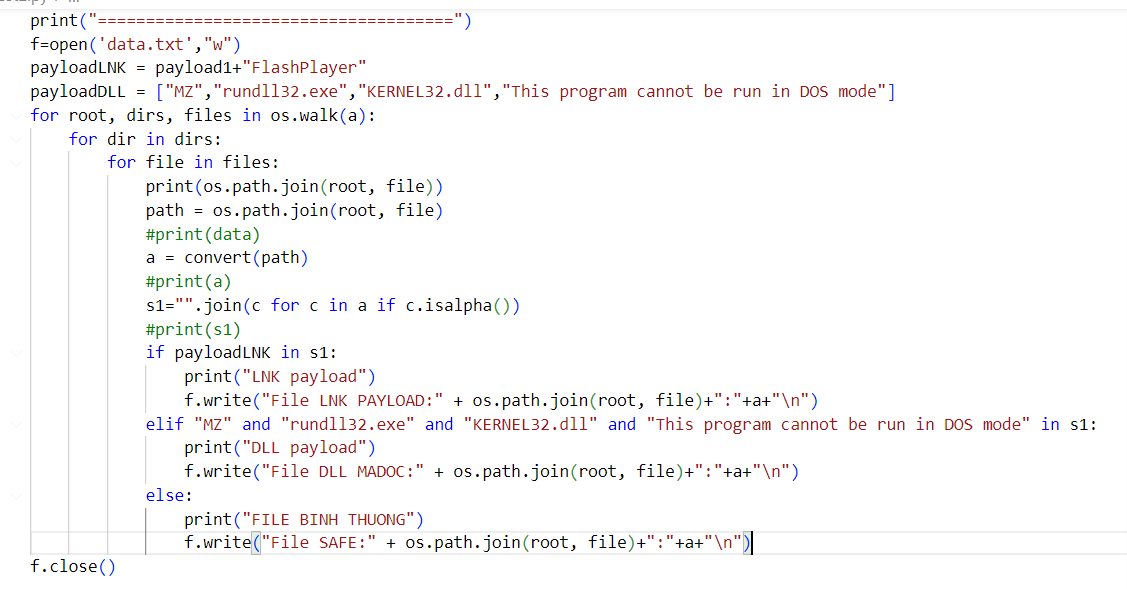
* Hàm **check** là hàm phát hiện usb đã kết nối vào máy và trả về tên của ổ đĩa usb



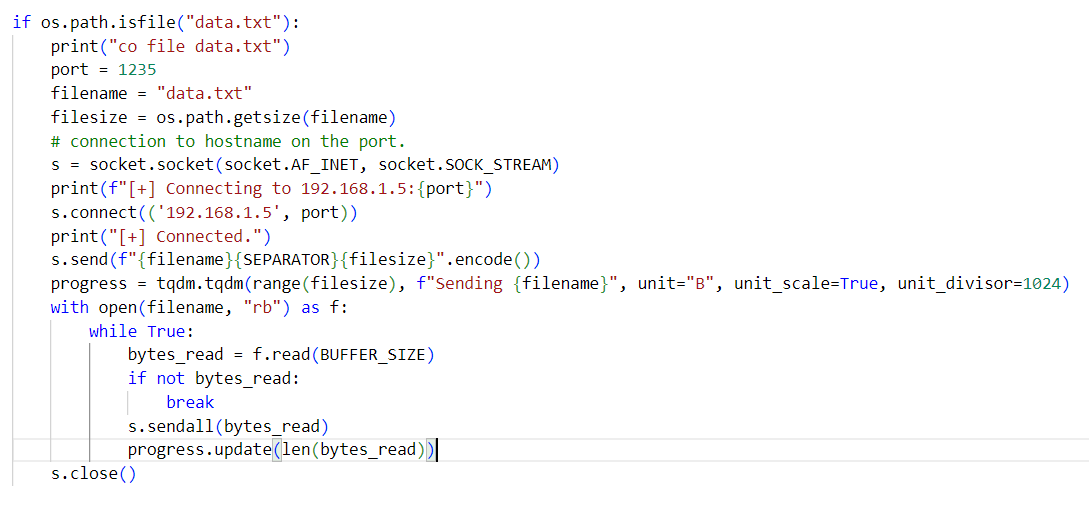
* Scan usb và lưu tất cả tên file trong usb ra file listfile.txt



* Scan tất cả file trong usb và phát hiện file lnk bị lỗi và file dll mã độc

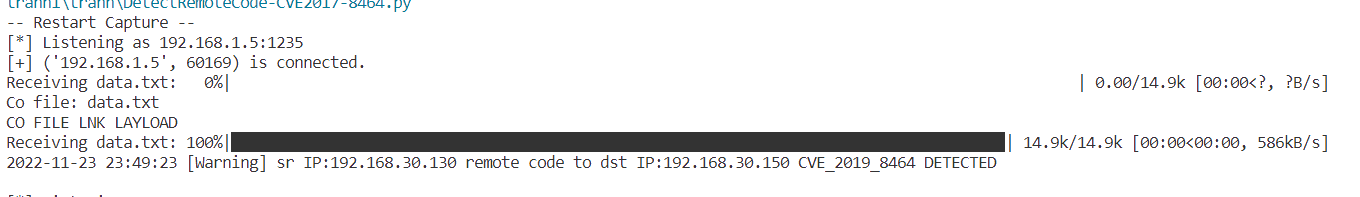


* Gửi kết quả phát hiện và dữ liệu của thấy cả các file

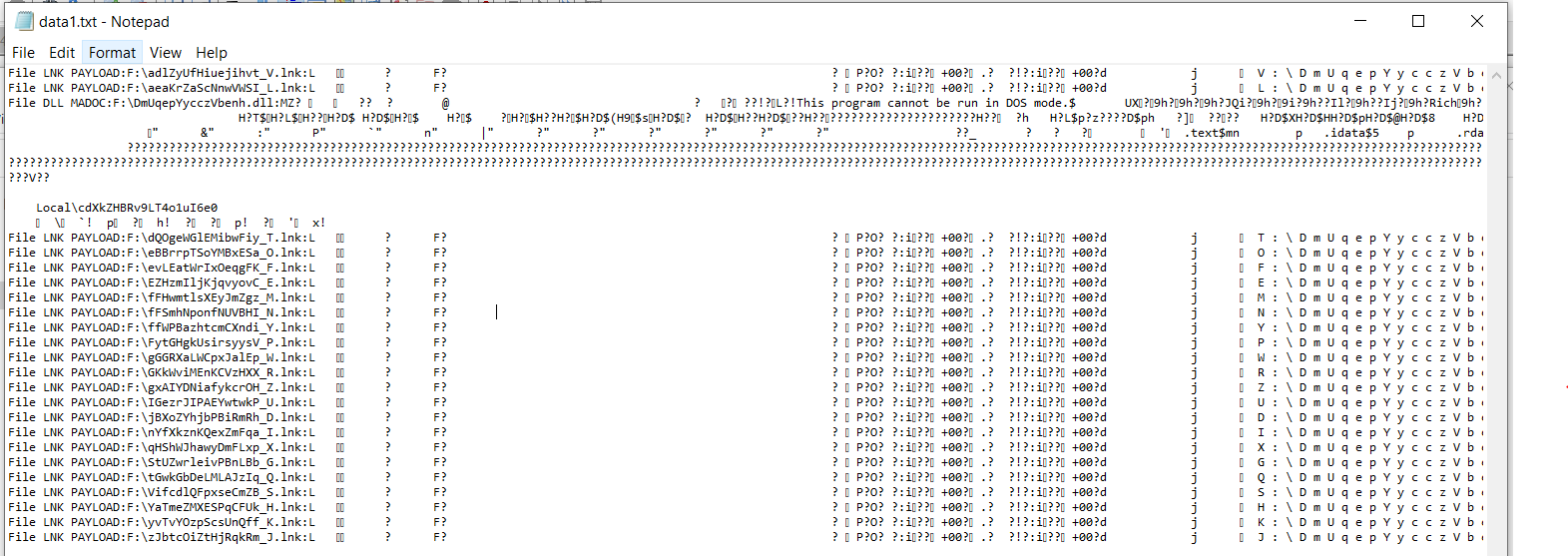


**\*Tiến hành kiểm tra hoạt động của chương trình qua thực hiện khai thác.**

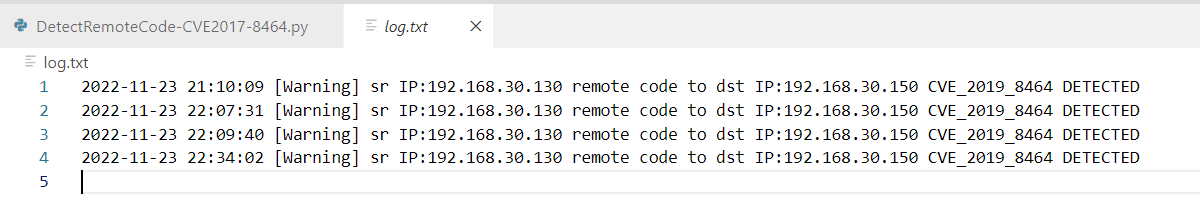
* Chạy chương trình giám sát trên máy windows 10 (máy thật) giám sát trên vùng mạng và chạy chương trình scan usb trên máy windows(victim) mà ta sẽ thực hiện lại tấn công như phần 2 ở trên.
* Quay lại 2 máy ảo và thực hiện lại các thao tác tấn công như phần 2. Ta thấy rằng lưu lượng mạng mà nó bắt được đã phân tích và phát hiện ra được kẻ tấn công đang thực hiện LNK Remote code được thông báo như hình bên dưới.
* Sau cùng muốn kết thúc quá trình dò quét trên cổng mạng chỉ cần bấm tổ hợp phím Ctr+C là ngặt chương trình chạy.



* Xem file data.txt mà client scan usb và truyền về server ta thấy có 23 file lnk và 1 file dll và dữ liệu trong các file đó và kết quả usb đã scan



* Sau đó kiểm tra file log.txt xem lại hoạt động vừa rồi có phát hiện gì không. Những phát hiện tấn công dựa trên CVE-2017-8464 nó cũng đã ghi nhận lại trong log với thời gian cụ thể và IP kèm theo như thông báo khi chạy chương trình.



**KẾT LUẬN**

Qua quá trình khai thác và xậy dựng chương trình phát hiện lỗ hổng CVE-2017-8464 hiểu được cách khai thác một lỗ hổng, từ đó phân tích ra được signature cũng như các hành vi hoạt động của mã độc trên lỗ hổng. Với việc phân tích hành vi và signature đó sẽ giúp người giám sát có khả năng tự viết chương trình để tự động thu thập, phân tích và xử lý thông tin giám sát an ninh mạng để đưa ra cảnh báo phát hiện mã độc.