BÁO CÁO BÀI TẬP

**Môn học:** Pháp chứng kĩ thuật số

**Tên chủ đề: MEMLABS**

*GVHD: Nghi Hoàng Khoa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT334.O21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |
| 2 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 3 | Nguyễn Ngọc Nhung | 21521248 | 21521248@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | MemLabs Lab 1 | 100% |
| 2 | MemLabs Lab 2 | 100% |
| 3 | MemLabs Lab 3 | 100% |
| 4 | MemLabs Lab 4 | 100% |
| 5 | MemLabs Lab 5 | 100% |
| 6 | MemLabs Lab 6 |  |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## Lab 1 - Beginner's Luck

**A screenshot of a computer

Description automatically generated**

* Đầu tiên, ta hãy tải challenge file về máy kali:

A screenshot of a computer

Description automatically generated

* Sau khi tải file thành công, chúng ta sử dụng volatility với plugin là imageinfo để xem thông tin:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

🡺 Profile được điều tra là Win7SP1x64.

* Theo mô tả **“we suddenly saw a black window pop up with some thing being executed.”** Có thể là màn hình cmd 🡺 thử kiểm tra các tiến trình được chạy với plugin pslist:

A screenshot of a computer

Description automatically generated A screenshot of a computer program

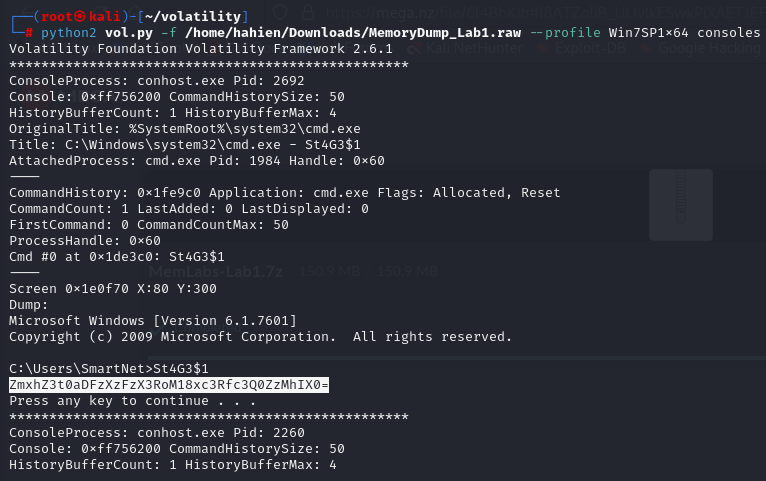
Description automatically generated

* Ta thấy tiến trình cmd.exe 🡺 dùng plugin cmdscan để kiểm tra:

A screenshot of a computer

Description automatically generated

* Phát hiện được 1 chuỗi: **St4G3$1**
* Dùngplugin consoles để kiểm tra rõ hơn về chuỗi này:



🡺 Ta phát hiện 1 chuỗi base64 encoded: **ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=**

* Giải mã base64 ta được:

A screenshot of a computer

Description automatically generated

🡺 **STAGE 1: flag{th1s\_1s\_th3\_1st\_st4g3!!}**

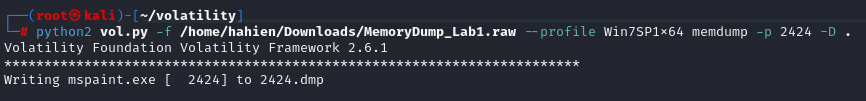
* Để tìm flag 2 thì ta tiếp tục dựa vào thông tin mô tả sau: **“When the crash happened, she was trying to draw something.”** Tiếp tục nhìn vào thông tin sau, ta thấy:

A screenshot of a computer program

Description automatically generated

🡺 Tiến trình PID=2424 mspaint.exe đang run.

* Thực hiện dump tiến trình này với plugin là memdump



* Thực đổi tên file từ 2424.dmp thành 2424.data

A close up of text

Description automatically generated

A black background with white text

Description automatically generated

* Mở file 2424.data với GIMP tool chỉnh thông số Width, Height của RGB image 🡺 cho tăng dần width đến khi thấy rõ được chữ gì đó, sau đó lật ngược ảnh ta có như sau:

A screenshot of a computer

Description automatically generated

🡺 **STAGE 2: flag{G00d\_BoY\_good\_girl\_}**

* Tiếp tục tìm kiếm flag của STAGE 3 🡺 Quay lại plugin pslist để thăm dò thêm các tiến trình đáng nghi:

A screenshot of a computer program

Description automatically generated

🡺 Có 1 tiến trình của WinRAR.exe khá nghi ngờ, với WinRAR thì thường có các file .rar, tiến hành kiểm tra xem:

A screen shot of a computer

Description automatically generated

* Dùng plugin dumpfiles với Offset tìm thấy, file sau khi dump thu được:

A screenshot of a computer

Description automatically generated

* Đổi định dạng file đã dump về dạng “.rar” để thực hiện được unrar

A screenshot of a computer

Description automatically generated

- Nhưng khi unrar thì file này cần nhập password và được gợi ý là NTLM hash in uppercase password tài khoản của Alissa

A screen shot of a computer

Description automatically generated

* Để xem được NTLM hash nên dùng plugin hashdump -> sau đó chuyển về dạng in hoa

A computer screen shot of a computer program

Description automatically generated

* Mở ảnh flag3.png để xem nội dung

A screenshot of a computer

Description automatically generated

🡺 **STAGE 3: flag{w3lL\_3rd\_stage\_was\_easy}**

## Lab 2 - A New World

**A screenshot of a computer

Description automatically generated**

* Đầu tiên, ta hãy tải challenge file về máy kali:

**A screenshot of a computer

Description automatically generated**

* Xem thông tin với plugin imageinfo:

A screenshot of a computer

Description automatically generated

* Với profile Win7SP1x64, thực hiện kiểm tra các tiến trình với plugin pslist:

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

* Có 3 điểm cần chú ý như sau:
  + He is supposedly a very popular "**environmental**" activist. (envars)
  + go to applications are **browsers**, his **password managers**.

🡺 Tiến trình cmd.exe, chrome.exe, KeePass.exe khả nghi

* Tiến trình cmd.exe run 🡺 thử với plugin cmdscan:

A screenshot of a computer

Description automatically generated🡺 Ở PID 2068 có chuỗi: Nothing here kids :)

* Sử dụng envars kiểm tra biến môi trường cho tiến trình 2068:

A screenshot of a computer

Description automatically generated

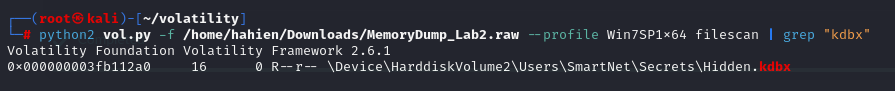
* Decode Base64 mã này xem sao: **ZmxhZ3t3M2xjMG0zX1QwXyRUNGczXyFfT2ZfTDRCXzJ9**

A screenshot of a computer

Description automatically generated

🡺 **STAGE 1: flag{w3lc0m3\_T0\_$T4g3\_!\_Of\_L4B\_2}**

* Để tìm ra flag tiếp theo thử kiểm tra tiến trình KeePass.exe (ứng dụng để lưu tài khoản và mật khẩu với định dạng là “.kdbx”)
* Sử dụng plugin filescan và tìm tất cả file chứa từ khóa “kdbx”:



* Với file Hidden.kdbx, thực hiện dumpfile để đọc được nội dung:

A screenshot of a computer

Description automatically generated

* Cài KeePass để có thể mở file:

A screenshot of a computer

Description automatically generated

* Mở ứng dụng KeePass và chọn mở file đã dump được ở trên thì nó yêu cầu 1 password

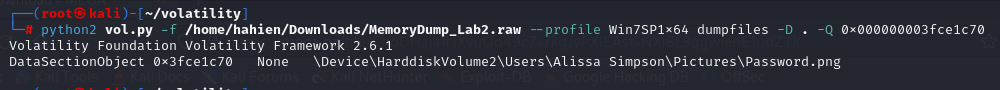
A screenshot of a computer

Description automatically generated

* Sử dụng plugin filescan và tìm với từ khóa “password” thì phát hiện 1 file Password.png 🡺 thực hiện dumpfile với offset đó.

A screen shot of a computer

Description automatically generated



A screen shot of a computer program

Description automatically generated

* Mở file .dat, phía góc cuối bên phải có 1 dòng Psst!! password is **P4SSw0rd\_123**

A screenshot of a computer

Description automatically generated

* Nhập **P4SSw0rd\_123** vào để mở được file .kdbx

A screenshot of a computer

Description automatically generated

* Xem các file trên KeePass để tìm kiếm các file chứa flag cần tìm:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

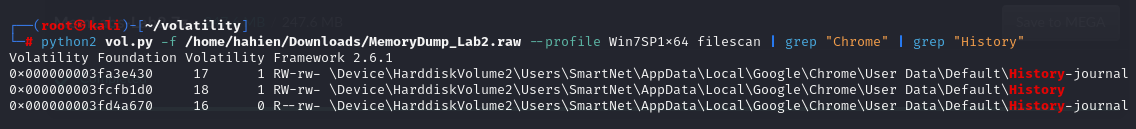
Description automatically generated

A screenshot of a computer

Description automatically generated

🡺 **STAGE 2: flag{w0w\_th1s\_1s\_Th3\_SeC0nD\_ST4g3\_!!}**

* Để tìm kiếm flag cuối cùng 🡺 thử xem xét về trình duyệt với các tiến trình chrome.exe 🡺 duyệt các file với filescan và tìm lịch sử duyệt web với 2 từ khóa là “Chrome” và “History”:

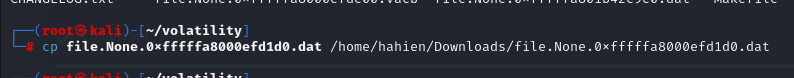


* Lịch sử duyệt web thường được lưu ở đường dẫn **AppData\Local\Google\Chrome\User Data\Default\History**
* Thực hiện dump thư mục trên với plugin là dumpfiles:

A screenshot of a computer program

Description automatically generated

* Mở file đã dump với DB Browser for SQLite để xem thông tin:



A screenshot of a computer

Description automatically generated

* Tại table urls, phát hiện 1 đường dẫn của mege.nz (nơi chia sẻ file trên internet)
* Copy đường dẫn và tìm kiếm:

A screenshot of a computer

Description automatically generated

* Giải nén và unzip file Important.zip nhưng nhận được gợi ý về password là SHA1 flag tìm được ở stage3 Lab1 dạng lowercase

A screen shot of a computer

Description automatically generated

* Với flag{w3lL\_3rd\_stage\_was\_easy} sử dụng sha1sum để hash và copy nhập vào password khi extract Important.zip:

A screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

* Đọc nội dung của file Important.png:

A screenshot of a phone

Description automatically generated

🡺 **STAGE 3: flag{oK\_So\_Now\_St4g3\_3\_is\_DoNE!!}**

## Lab 3: The Evil's Den

A screenshot of a computer

Description automatically generated

* Xem thông tin file dump.

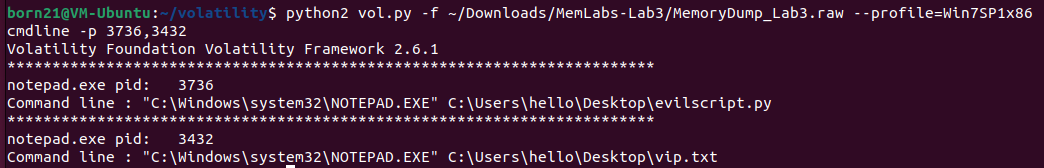
A computer screen shot of a program

Description automatically generated

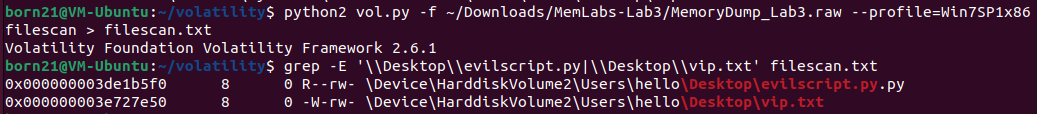
* Đầu tiên, kiểm tra các tiến trình đang chạy bằng plugin pstree.



* Hiện có hai quy trình của chương trình notepad.exe đang chạy trên máy tính với các ID quy trình (Pid) là 3736 và 3432. Bằng cách sử dụng plugin cmdline, có thể xem được các tập tin cụ thể đã được mở bằng các phiên bản của chương trình notepad.exe này.



* Notepad đang mở 2 tệp evilscript.py và vip.txt. Để xem nội dung của 2 file, trước tiên, sử dụng plugin filescan để quét thông tin 2 file này.

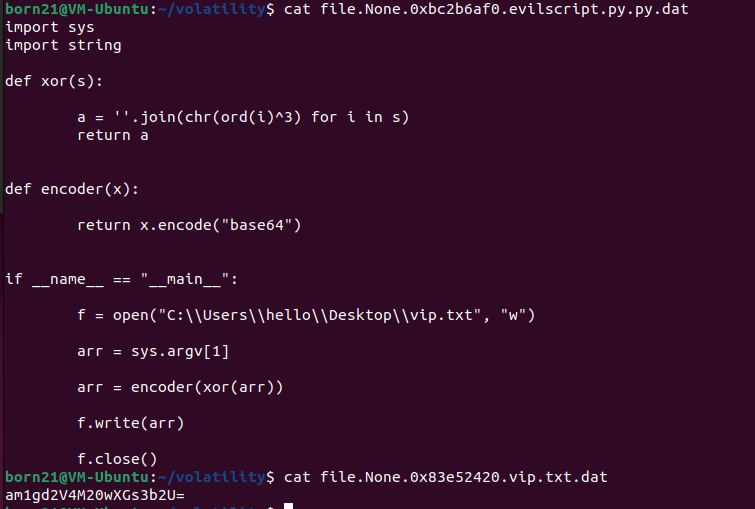


* Biết được offset của 2 file, ta tiến hành dumpfiles.

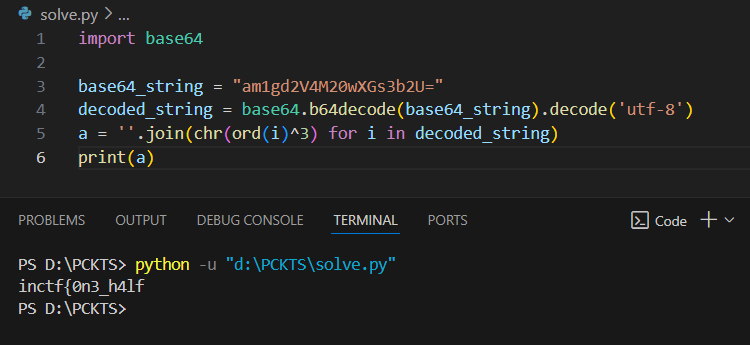
A computer screen shot of text

Description automatically generated

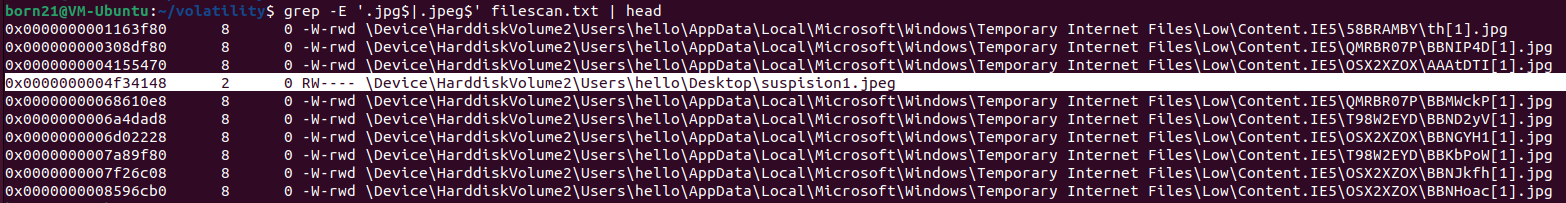
* Đọc nội dung 2 file vừa dump.



* Đoạn code trong file evilscript.py thực hiện mã hoá một chuỗi input bằng cách xor mỗi kí tự trong chuỗi với 3, sau đó mã hoá base64 và ghi vào tệp vip.txt
* Để biết được chuỗi input ban đầu, ta tiến hành đảo ngược quá trình trên.



* Ta có được 1 phần của flag: inctf{0n3\_h4lf
* Từ gợi ý steghide của đề bài, chúng ta sẽ scan những định dạng tệp hình ảnh phổ biến.



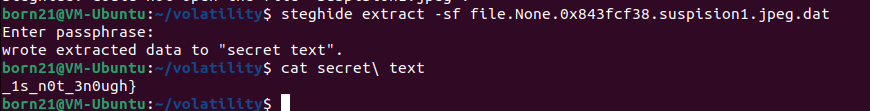
* Trong kết quả trả về có 1 tệp khá đặc biệt nên chúng ta sẽ dump file này để xem nội dung.



* File thu được:

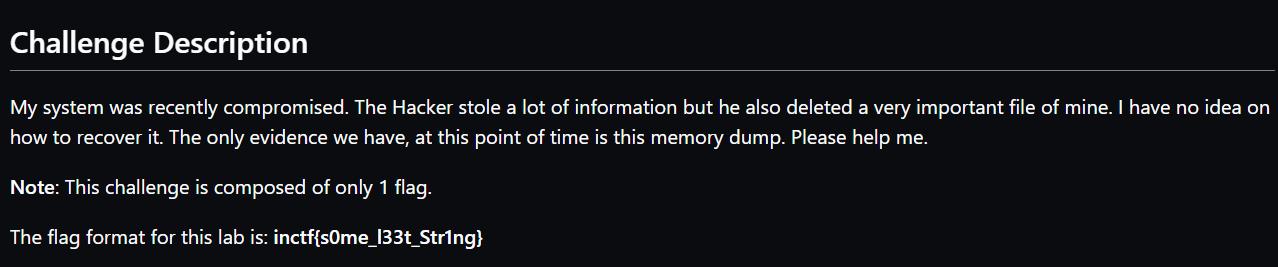


* Không có thông tin gì ở đây, chúng ta có thể dùng steghide để kiểm tra xem có nội dung nào được ẩn hay không.

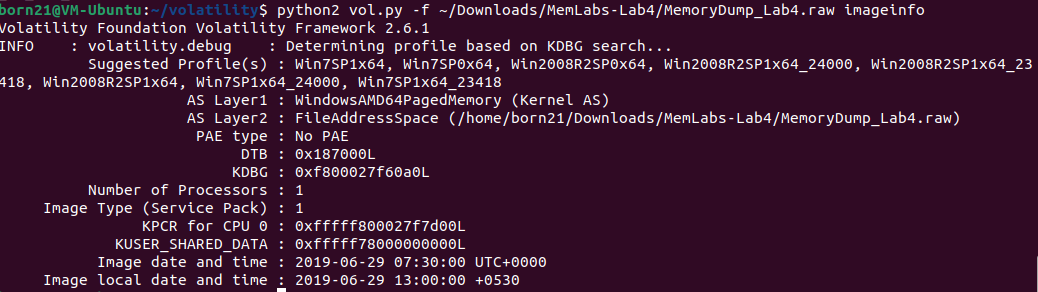


* Password là 1 phần của flag đã giải trước đó. Ta biết được phần còn lại của flag.
* Flag: inctf{0n3\_h4lf \_1s\_n0t\_3n0ugh}

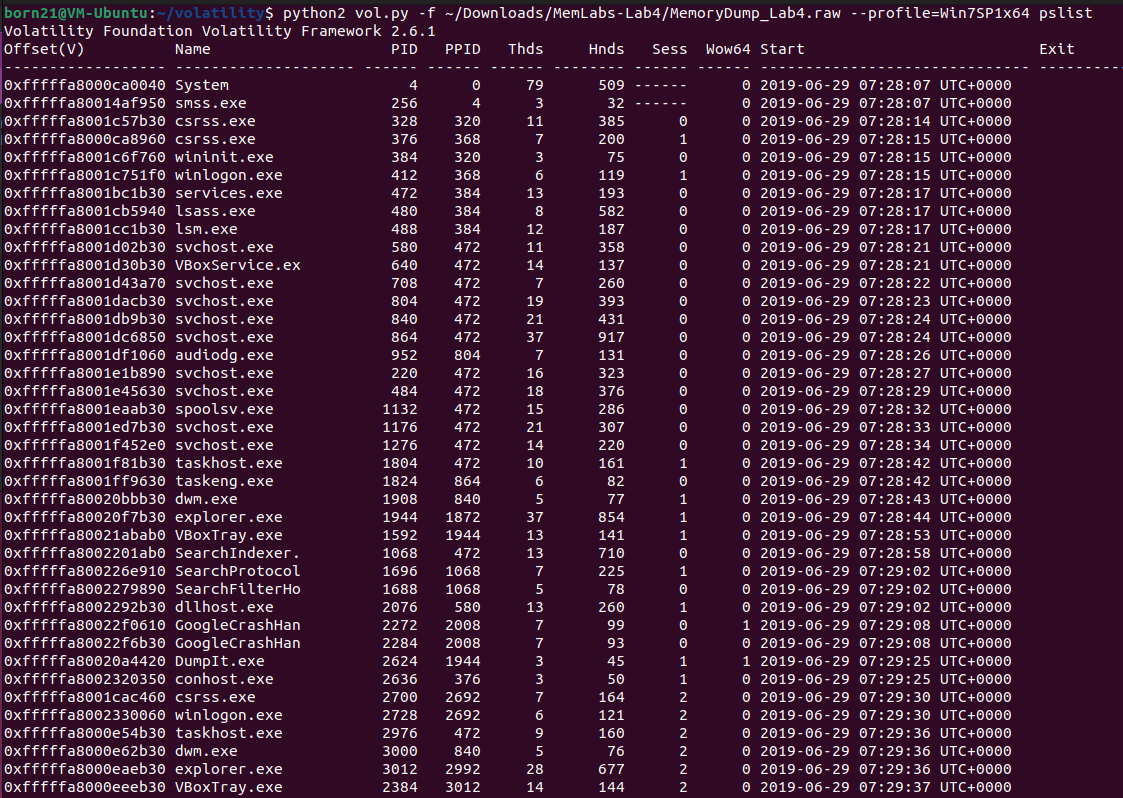
## Lab 4: Obsession



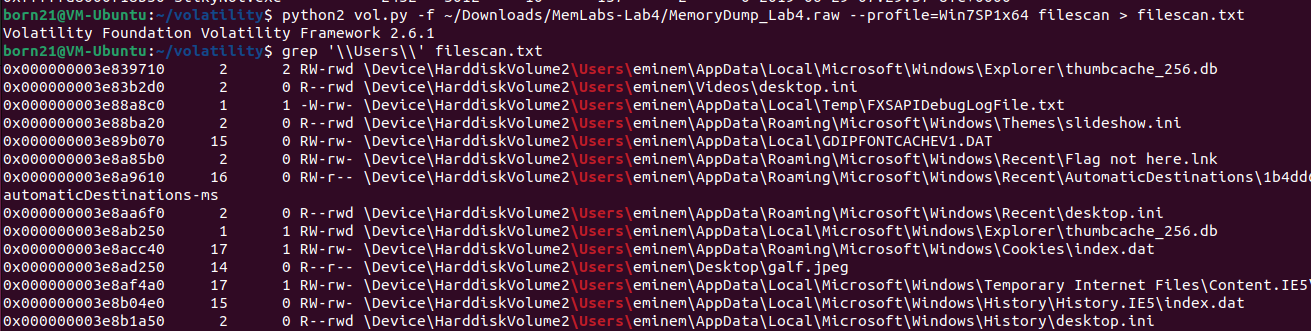
* Xem thông tin file dump.



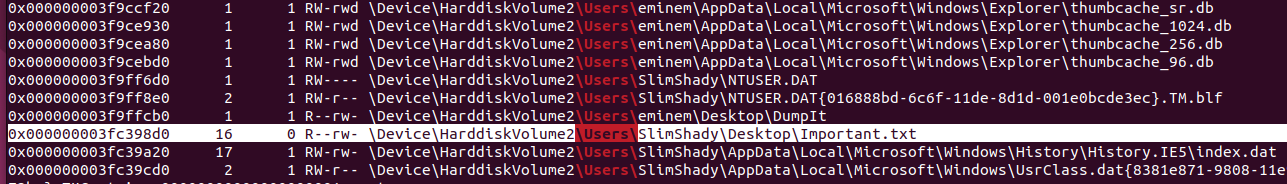
* Kiểm tra các tiến trình đang chạy.



* Không khai thác được thông tin gì từ các tiến trình. Từ gợi ý đề bài là file đã bị xoá, chúng ta hãy thử filescan. File rất quan trọng đối với người dùng có thể sẽ được lưu trong thư mục User nên sẽ lọc ra các tệp ở trong thư mục này.



* Chú ý vào file sau:

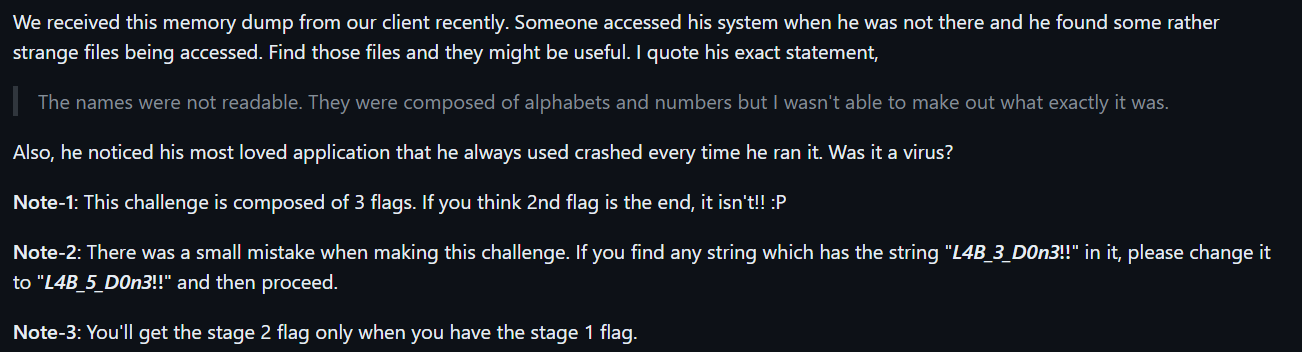


* Thử dumpfile để xem nội dung nhưng không có ou

Đoan

## Lab 5: Black Tuesday

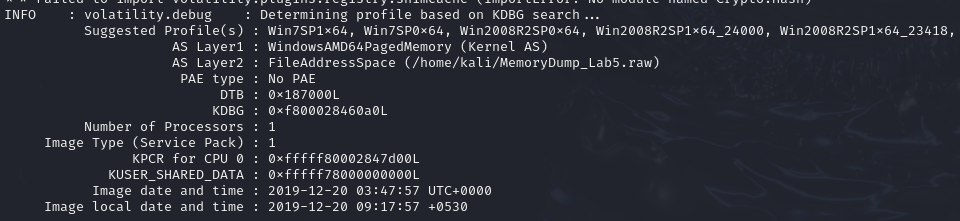
* Mô tả challenge:



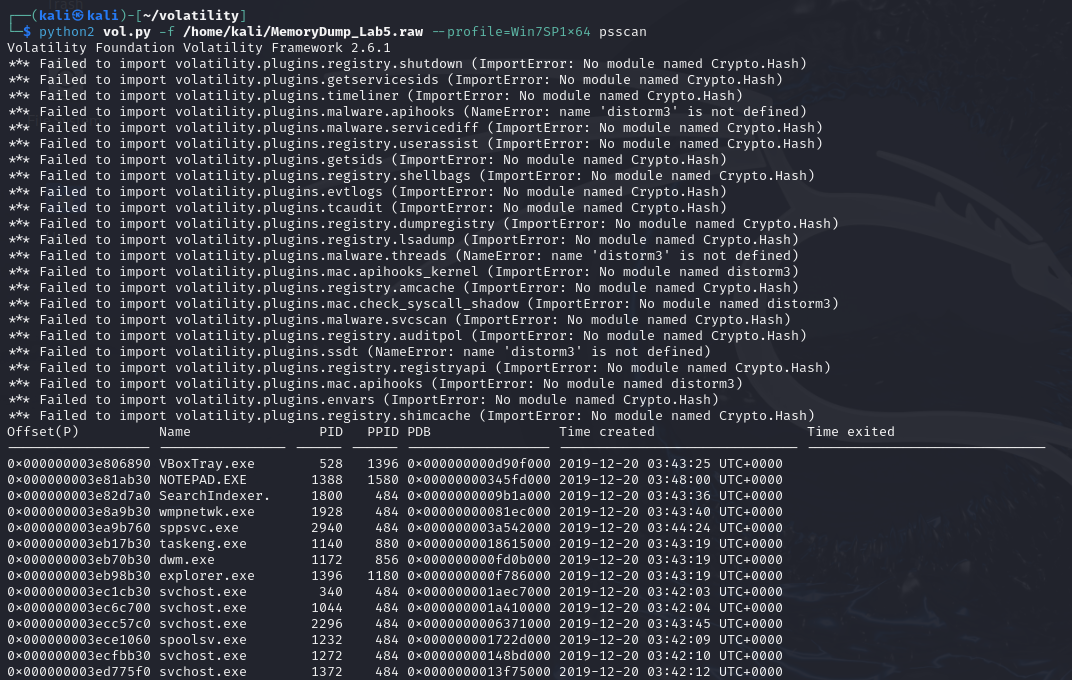
Gần đây chúng tôi đã nhận được kết xuất bộ nhớ này từ khách hàng của mình. Ai đó đã truy cập vào hệ thống của anh ấy khi anh ấy không có ở đó và anh ấy phát hiện thấy một số tệp khá lạ đang được truy cập. Tìm những tập tin đó và chúng có thể hữu ích. Tôi trích dẫn chính xác tuyên bố của anh ấy, Những cái tên không thể đọc được. Chúng bao gồm các bảng chữ cái và số nhưng tôi không thể biết chính xác nó là gì. Ngoài ra, anh ấy còn nhận thấy ứng dụng yêu thích nhất mà anh ấy luôn sử dụng bị lỗi mỗi khi chạy nó. Đó có phải là virus không?

Lab 5 có 3 flags.

* Sau khi tải và giải nén, được 1 tập tin raw. Em sử dụng plugin imageinfo để kiểm tra thông tin của file dump:

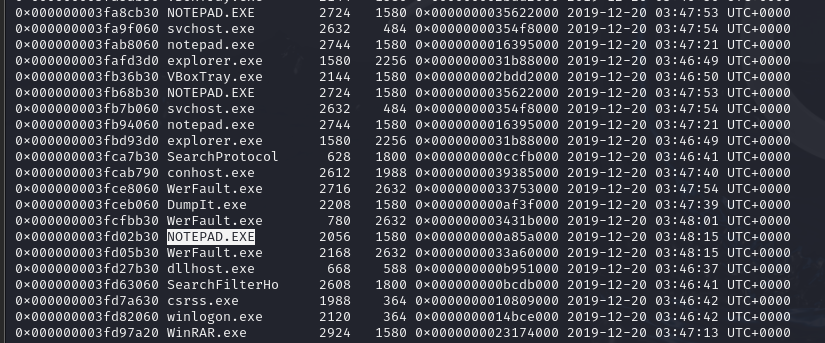


* Dùng *psscan* để kiểm tra các process đang chạy:

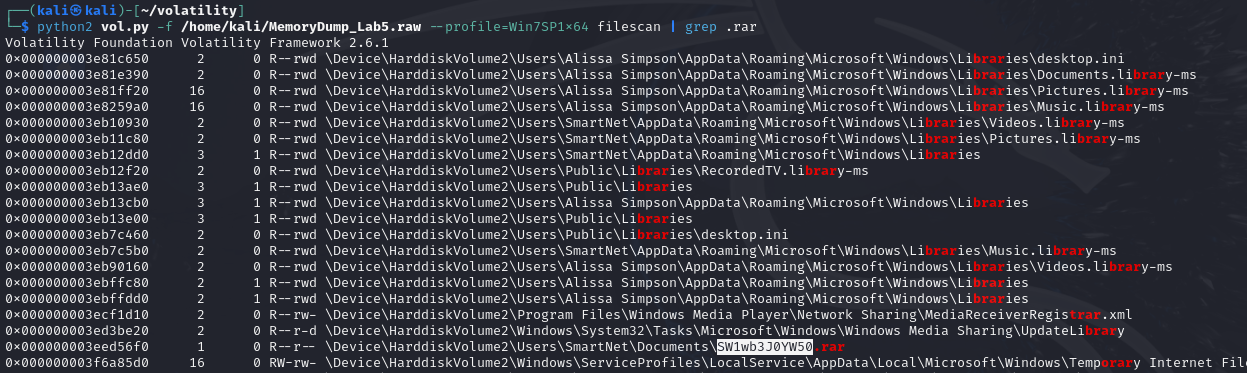


Do em cài lại máy ảo nên lỗi Crypto.Hash em chưa kịp fix, để dễ quan sát thì em sẽ chỉ chụp kết quả sau khi chạy plugin chứ không chụp lại câu lệnh ạ.

Lướt xuống phía dưới, em tìm thấy 2 ứng dụng quen thuộc là NOTEPAD và WinRAR:

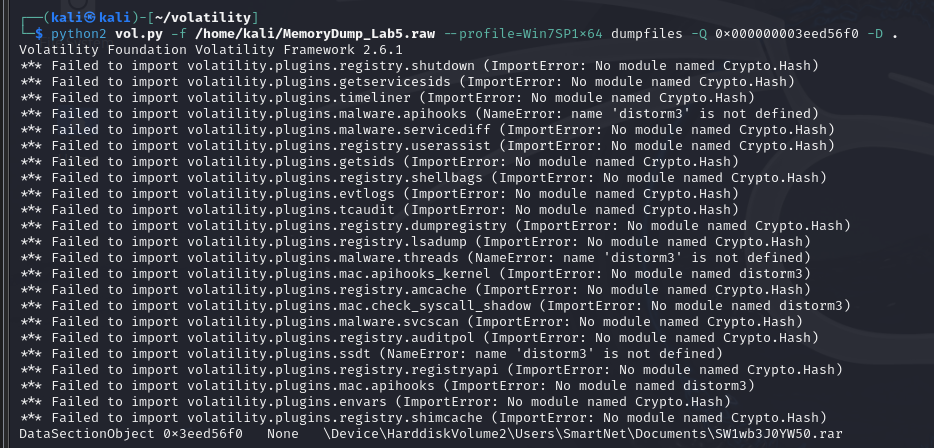


* Do đó, em sẽ tìm file .rar bằng *filescan | grep .rar*:

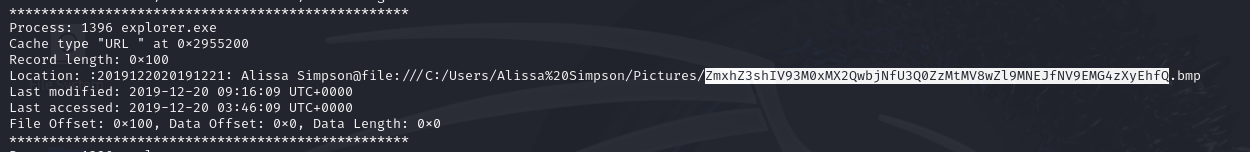


Có một file với tên kỳ lạ, đọc vào không hiểu rõ đó là file gì.

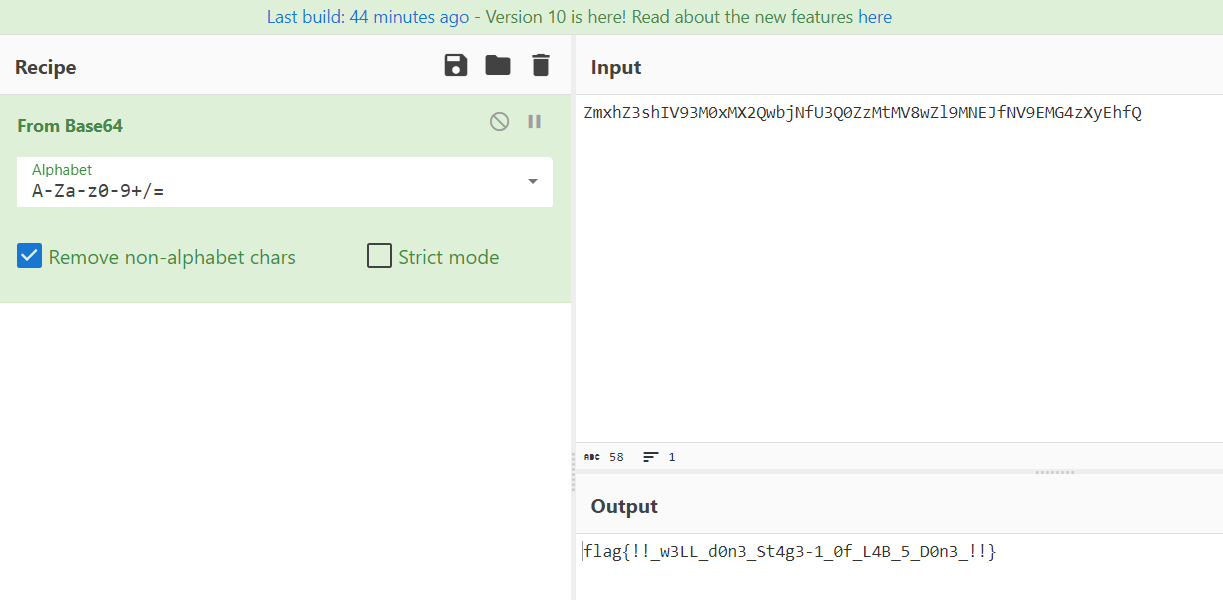
* Để xem rõ về file .rar trên, em sẽ dùng *dumpfile:*



* Sau khi dump thì được 1 file nén. Tuy nhiên nó cần password để mở. Em thực hiện tiếp để tìm password đầu tiên.
* Kiểm tra lịch sử duyệt web bằng *iehistory*, em tìm được đoạn mã đang ngờ:

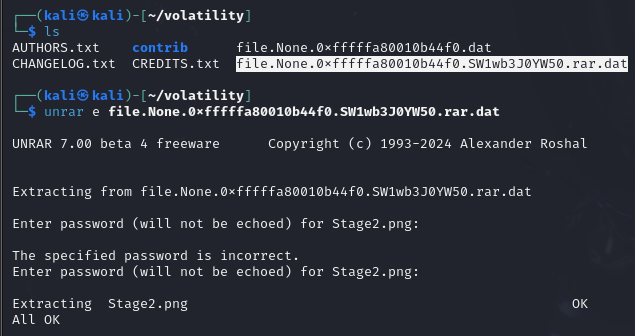


* Em decode đoạn mã trên bằng CyberChef, thành công tìm được cờ đầu tiên:

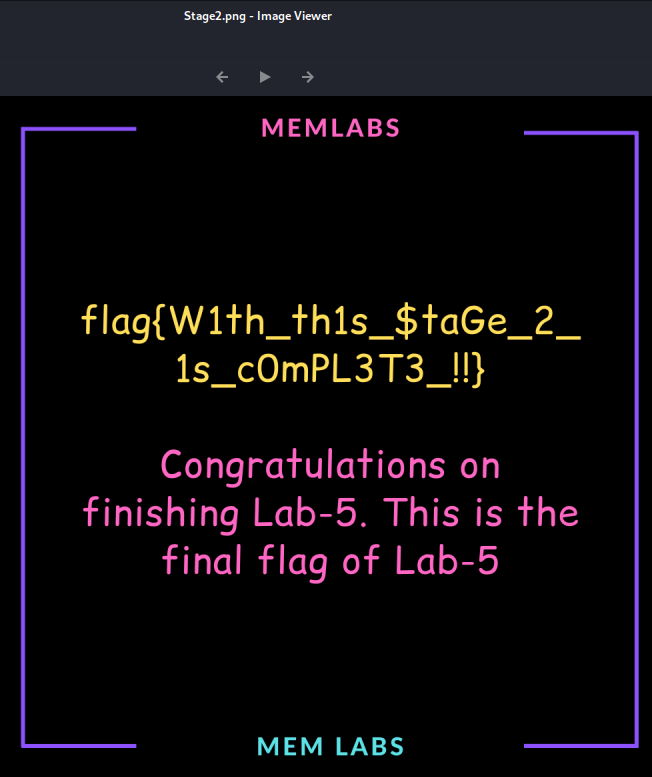


## flag{!!\_w3LL\_d0n3\_St4g3-1\_0f\_L4B\_5\_D0n3\_!!}

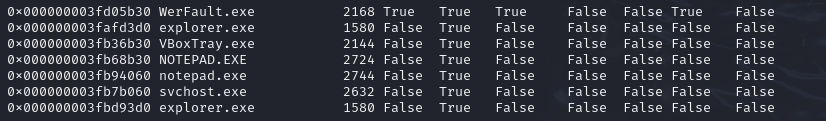
* Flag trên chính là password cần tìm, nhập vào thì đã extract được 1 file ảnh png:



Và flag thứ 2 là

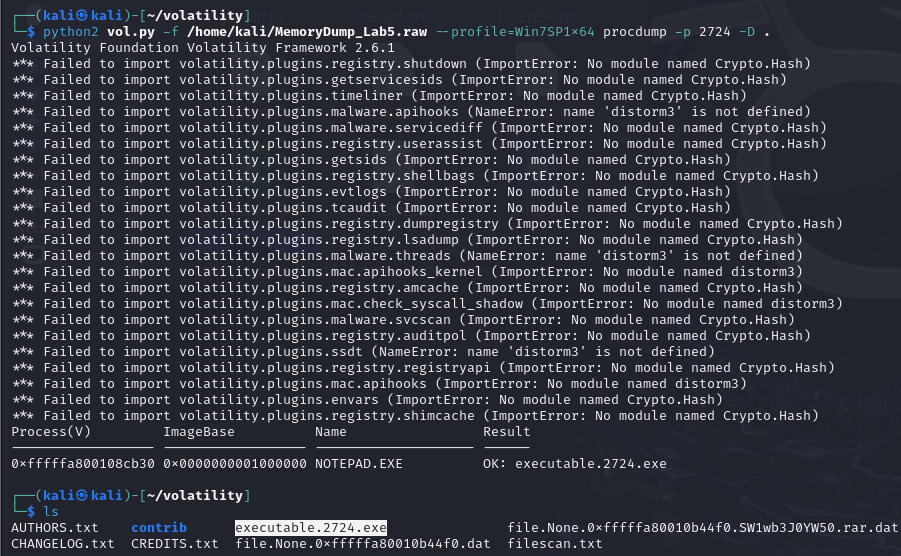


* Tuy nhiên, đề yêu cầu 3 flag, nên tìm tiếp flag cuối cùng, em sẽ xử lý tiếp NODEPAD.exe. Dùng psxview để xem các quá trình ẩn trên hệ thống:



NODEPAD có nhiều tiến trình, tuy nhiên do đề có nói truy cập nhưng không sử dụng được, nên em sẽ chọn tiến trình bị false nhiều nhất có PID là 2724.

* Sử dụng procdump:



## Lab 6: The Reckoning

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)