BÁO CÁO CUỐI KỲ

**Môn học: Pháp chứng kỹ thuật số**

# **Nhóm:** Pha pha

**THÀNH VIÊN THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Nguyễn Đoàn Xuân Bình | 19521265 |
| 2 | Trần Hoàng Khang | 19521671 |
| 3 | Nguyễn Mỹ Quỳnh |  |

**NOTE: Các bước tìm loại profile thích hợp bằng plugin imageinfo sẽ không liệt kê vào đây. Nó rất cơ bản.**

## King of Memory Forensics

Description:

My laptop was stolen and the police found it. Unfortunately before it was stolen I forgot to set a password for my laptop. So the thief added the password and left something inside my laptop. Can you find those?

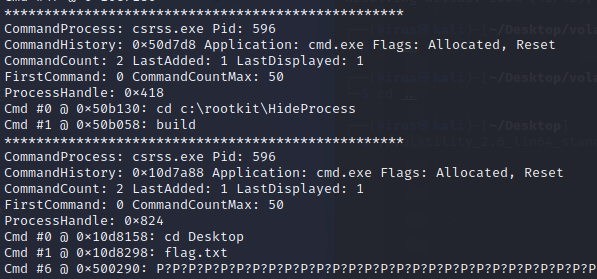
Format Flag: W1{PasswordLaptop-ProcessIsHidden-Message-WhatDoesTheMaliciousCodeShow?}

- - -

Với flag có định dạng 4 mảnh như trên. Mình sẽ tìm lần lượt theo các keyword trên, theo thứ tự mình tìm ra được

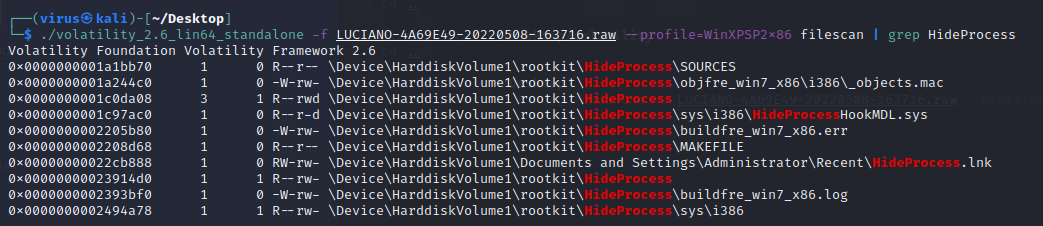
A. Đầu tiên mình theo từ khóa **Message:**

Thật ra thì tại đây mình không có thông tin gì nhiều. Nhưng mà trước đó có từ khóa **ProcessIsHidden** và **WhatDoesTheMaliciousCodeShow** nên khả năng là có một con malware ở đây. Do vậy nên mình sẽ dùng **cmdscan** để xem chung chung vì attack sẽ dùng lệnh để thao tác cài con này lên.



Ta thấy có thư mục ***c:\rootkit\HideProcess***. Tìm thử với từ khóa này và vét bằng **filescan**

|  |
| --- |
| ./volatility\_2.6\_lin64\_standalone -f LUCIANO-4A69E49-20220508-163716.raw --profile=WinXPSP2x86 filescan | grep HideProcess |



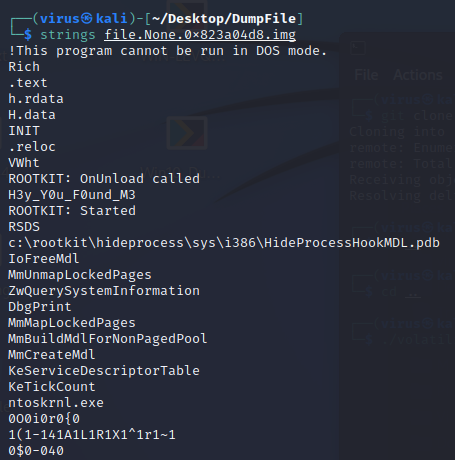
Dump từng file từng file một bằng **dumpfiles** và sử dụng strings để lấy chuỗi cần thiết (ta sẽ thấy trong này là những file sau khi con rootkit được build và chạy). Tạo folder **DumpFile**

|  |
| --- |
| mkdir DumpFile |

Thử từng file bằng cách trên cho đến khi file **HideProcessHookMDL.sys** với địa chỉ ảo tại *0x0000000001c97ac0* , ta thấy có xuất hiện định dạng flag

|  |
| --- |
| ./volatility\_2.6\_lin64\_standalone -f LUCIANO-4A69E49-20220508-163716.raw --profile=WinXPSP2x86 dumpfiles -Q 0x0000000001c97ac0 -D DumpFile |

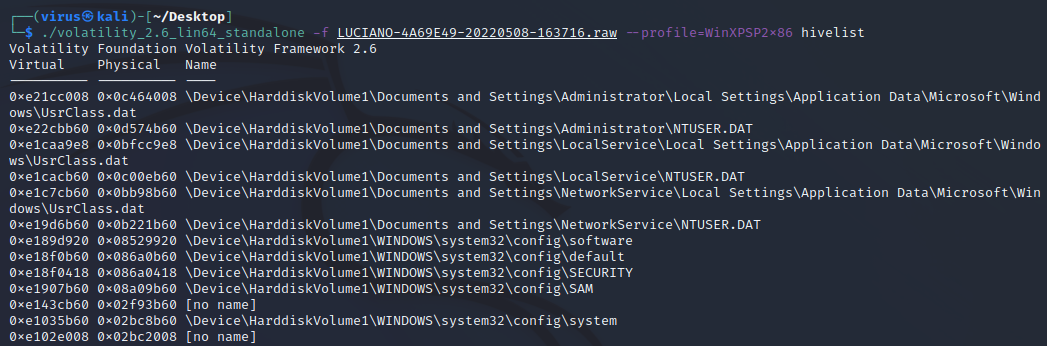
Và đó là một mẩu



Flag: **H3y\_Y0u\_F0und\_M3**

B. Tiếp theo mình theo từ khóa **PasswordLaptop:**

Thử tìm hash password bằng cách thông thường, dùng plugins **hivelist** :



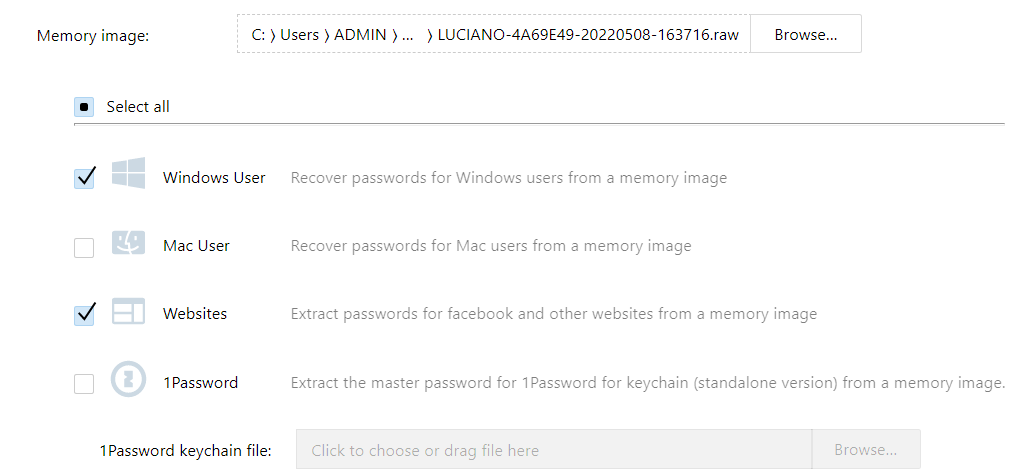
Ta thấy thông tin hive (registry) bị thay đổi và không còn key đầu vào của \REGISTRY\MACHINE\SYSTEM thì việc trích xuất hash là bất khả thi.

Tiếp theo dump bằng **lsadump** để xem các credential nhạy cảm nhưng cũng không ra, vì nó bản chất sẽ dump các thông tin từ trong các tiến trình liên quan, các storage và trong registry để lấy giá trị như khóa (key) hay default password , …

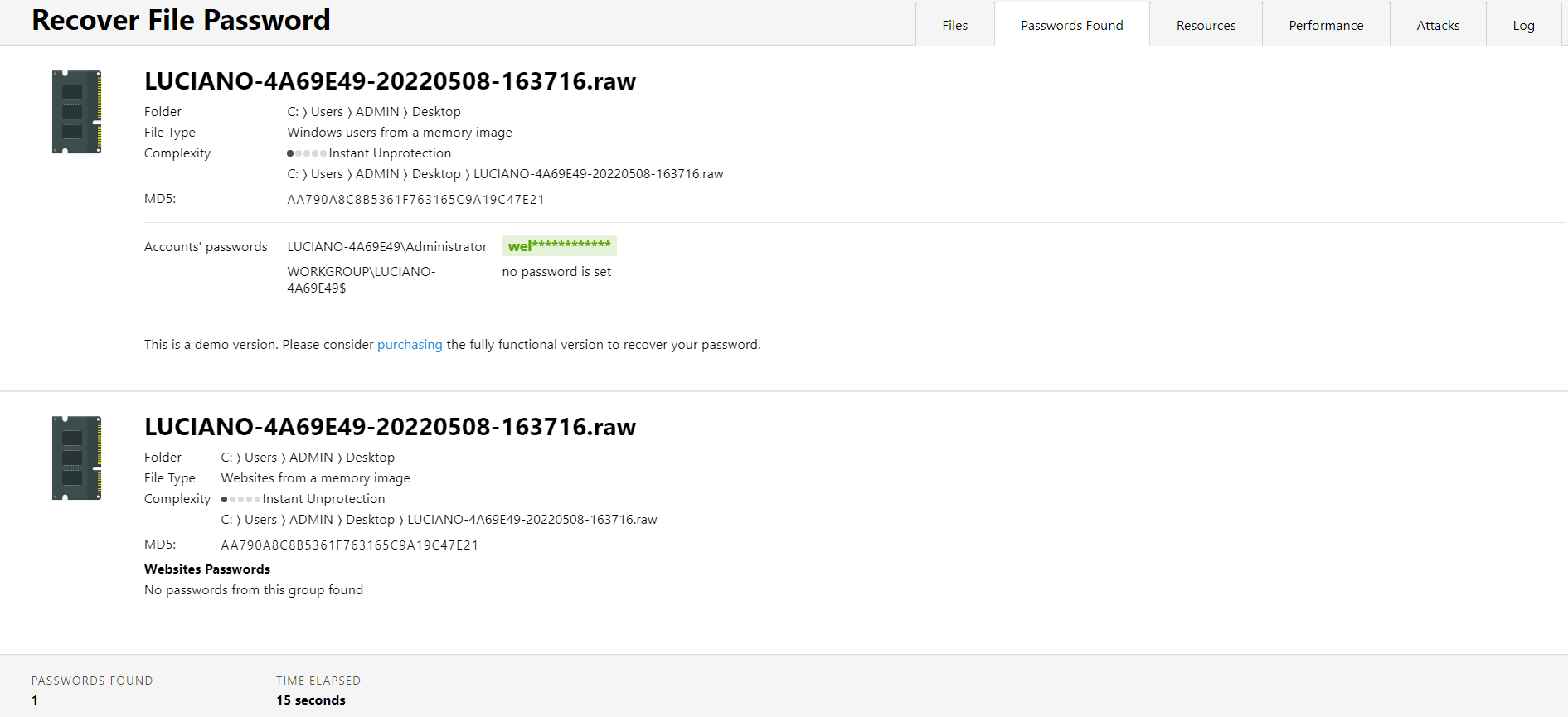
Chuyển sang dùng plugin bên ngoài là **mimikatz** và tích hợp vào Volatility cũng không mang lại kết quả.

Chuyển sang dùng tool **Passware Kit Forensic.**

Vào *Memory Analysis* 🡪 Cấu hình scan như sau :



Scan để tìm password



Vào tab Attacks thì thấy một tài khoản *welcometow1* chưa được set password

## 2. King of Stegano (300)

Description:

My picture is corrupted

My zip file lost password

So sad :((

- - -

Text

Description automatically generated

Khi mở file ảnh Chall.png lên thì file ảnh bị lỗi.

Graphical user interface, text, application, table

Description automatically generated

Em dùng HxD để xem file ảnh thì thấy file ảnh PNG mà thiếu phần header và phần footer nên em thêm Header và footer vào.

Graphical user interface, application, table, Excel

Description automatically generated

Sau khi thêm header.

Graphical user interface, application, table, Excel

Description automatically generated

Sau khi thêm footer thì ta được hình ảnh như sau.

A picture containing mammal, bovine, horse

Description automatically generated

Sau khi recovery được hình này thì em dùng tool appa để tìm flag được ẩn trong đó.

Text

Description automatically generated

Kết quả em sẽ được một nữa flag như sau: W1-Y0u-4r3

Text

Description automatically generated

Tiếp theo với tệp CrackMe.zip mà challenge cho thì tệp này được set password nên không thể truy cập. Vì thế em sử dụng một kiểu tấn công là known-plaintext-attack để tìm flag còn lại.

Ở đây thì em sử dụng tool pkcrack để thực hiện tấn công.

Link github của tool này đây: <https://github.com/keyunluo/pkcrack>

Tiếp theo em đem ảnh em vừa recovery ở trên sang kali để zip nó lại thành file chall.zip

A screenshot of a computer

Description automatically generated with medium confidence

Tiếp theo thì em chạy tool pkcrack để tạo ra một file zip không có mã hóa như sau.

Text

Description automatically generated

Đây là kết quả sau khi tool chạy xong.

Text

Description automatically generated

Thì trong thư mục em được file zip không mã hóa này.

A screenshot of a computer

Description automatically generated with low confidence

Graphical user interface, text, application

Description automatically generated

Và đây là flag: -K1ng-0f-F0r3ns1cs

Flag cuối cùng là : **W1-Y0u-4r3-K1ng-0f-F0r3ns1cs**