BÁO CÁO BÀI TẬP

**Môn học: Pháp chứng kỹ thuật số**

**Session: King of Memory Forensics**

*GVHD: Nghi Hoàng Khoa*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT334.O21.ATTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 2 | Hà Thị Thu Hiền | 21522056 | 21522056@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 | Kịch bản 1 | 100% |

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

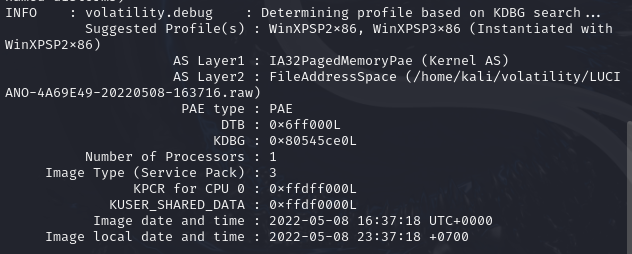
BÁO CÁO CHI TIẾT

**Mô tả:** Máy tính xách tay của tôi gần đây đã bị đánh cắp và may mắn thay, nó đã được cảnh sát thu hồi. Đáng tiếc là tôi đã không đặt mật khẩu cho máy tính xách tay của mình trước khi nó bị mất trộm. Kẻ đánh cắp nó đã cài đặt mật khẩu và có khả năng đã đặt các tệp hoặc phần mềm trên thiết bị. Bạn có thể hỗ trợ truy cập vào máy tính xách tay và xác định bất kỳ bổ sung trái phép nào không?

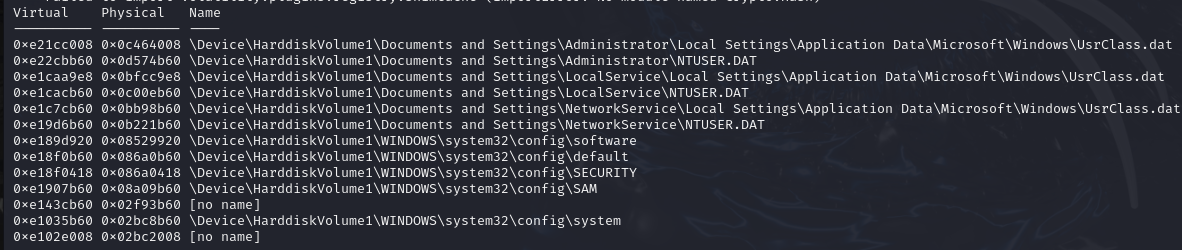
Format Flag: W1{PasswordLaptop-ProcessIsHidden-Message-WhatDoesTheMaliciousCodeShow?}

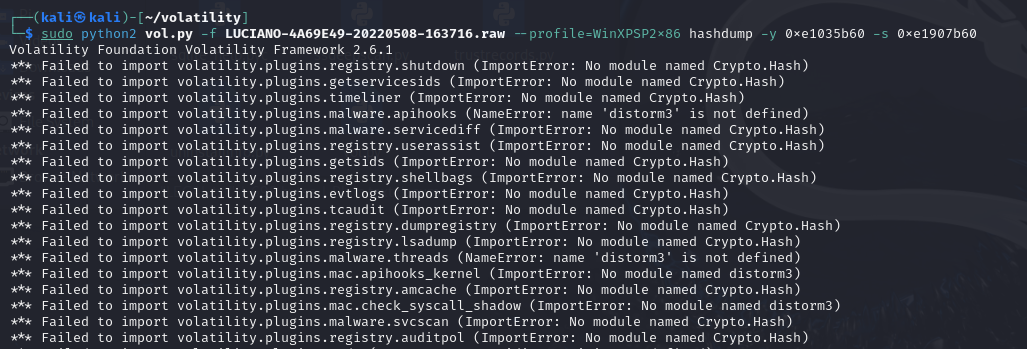
**Đáp án:**

* + Dùng plugin *imageinfo* tìm profile cho file dump:

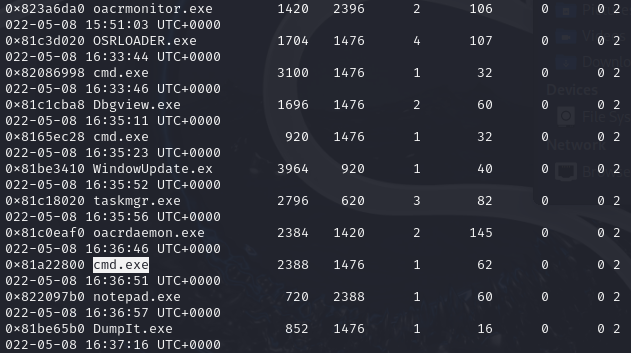


* Tìm password:
* Do máy tính đã cài mật khẩu, và flag cũng cần có mật khẩu nên em dùng *hivelist + hashdump* để tìm password. Tuy nhiên không có kết quả:

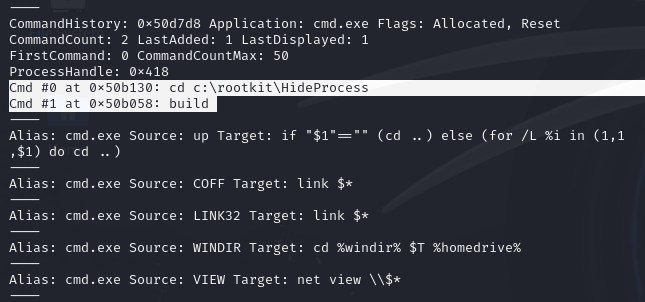




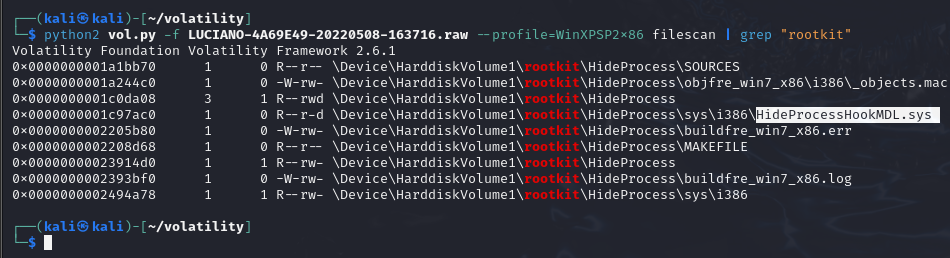
* Em dùng *Passware Kit Forensics* - một phần mềm chuyên bẻ khóa mật khẩu. Nhưng có tính phí, do đó em dùng bản crack, tìm được password là *welcometow1.*
  + Dùng *pslist* và xem các tiến trình đang chạy, *cmd.exe* được mở nhiều lần:



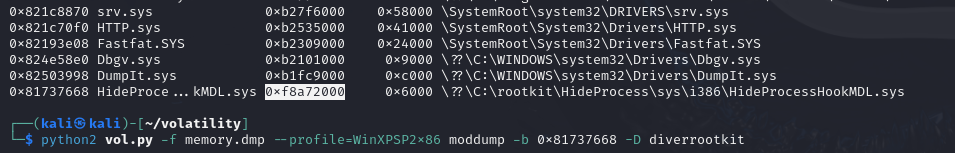
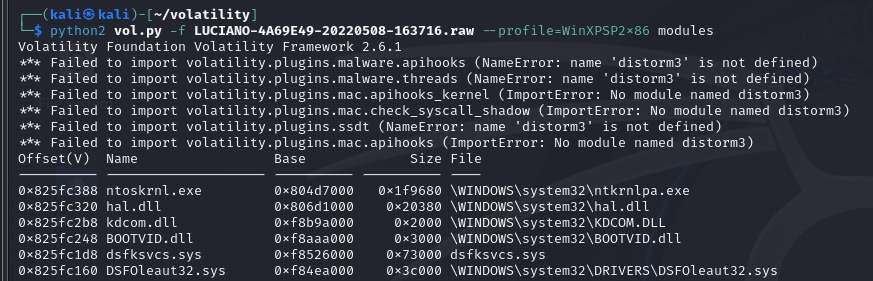
* + Dùng plugin *consoles* và xem lịch sử dòng lệnh. Có rootkit đã được build và ẩn process:



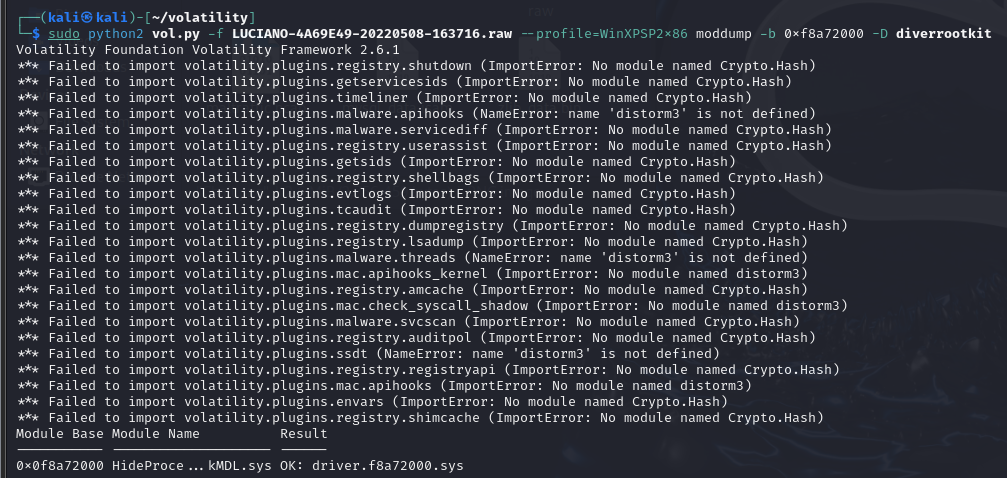
* Tiến hành tìm các file có liên quan đến từ khóa rootkit:



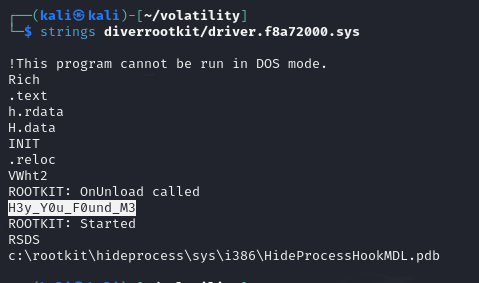
* Chạy *modules* và tìm địa chỉ bắt đầu của driver này*:*



* Sử dụng plugin *moddump* để dump driver *HideProcessHookMDL.sys*:

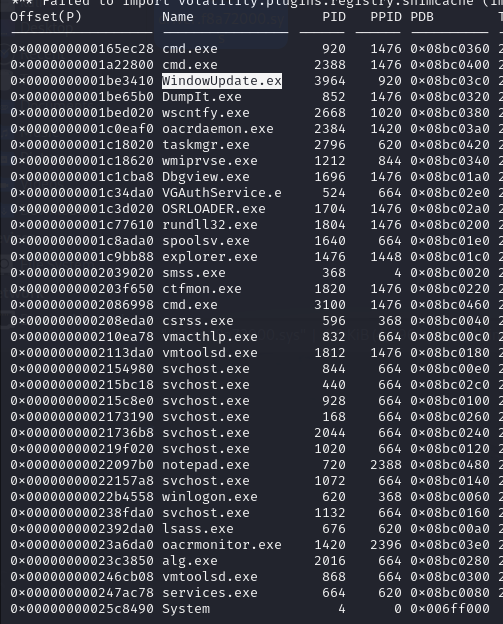


* Tìm chuỗi trong file kết quả vừa dump được, em tìm được chuỗi có nghĩa sau:



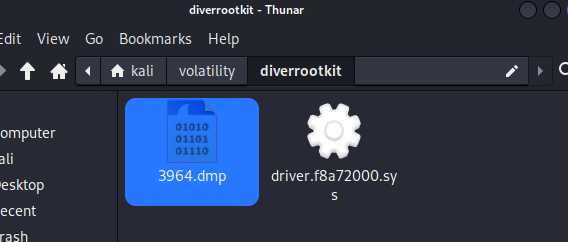
Message: **H3y\_Y0U\_F0und\_M3**

* Tìm tiến trình ẩn:
  + Dùng *psscan* liệt kê cả tiến trình ẩn. Có tiến trình *WindowUpdate.exe* có thể là tiến trình cần tìm vì nó thực hiện các thay đổi trên máy tính của user:



* + WindowUpdate có PID là 3964, em sẽ dump file và tìm strings độc hại trong file dump:

*python2 vol.py -f LUCIANO-4A69E49-20220508-163716.raw --profile=WinXPSP2x86 memdump -p 3964 -D driverrootkit/*



* + Tìm được chuỗi độc hại với từ khóa “malware”:



* Vậy có thể kết luận, tiến trình ẩn là *WindowUpdate* và nội dung đoạn code độc hại show là “*easy\_malware\_detection*”.
* Tổng kết: flag là:

**W1{welcometow1-WindowUpdate-H3y\_Y0U\_F0und\_M3-easy\_malware\_detection}**

---

***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)