BÁO CÁO THỰC HÀNH

**Môn học: Pháp chứng kỹ thuật số**

**Lab 1:**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT522.N11.ATCL.1

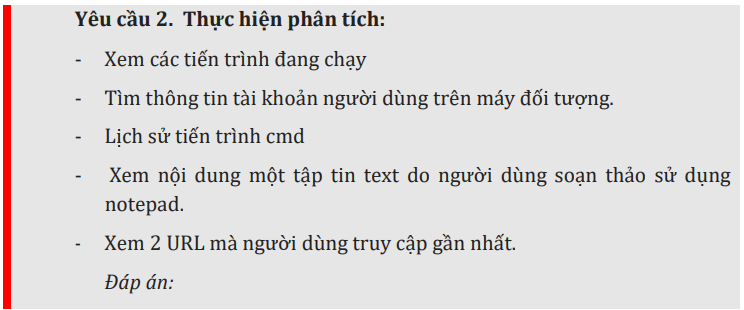
|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Văn A | 1952xxxx | 1952xxxx@gm.uit.edu.vn |
| 2 | Nguyễn Văn B | 1952xxxx | 1952xxxx@gm.uit.edu.vn |

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Bài tập 1 | 100% |
| 2 | Bài tập 2 | 100% |
| 3 | Bài tập 3 | 100% |

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

BÁO CÁO CHI TIẾT



Thông tin file : WIN-LEVQF1CLMR1-20181126-091622

A screenshot of a computer

Description automatically generated

* **Xem các tiến trình đang chạy**

Để tìm kiếm các tiến trình đang chạy, ta sử dụng lệnh psscan hoặc pslist để liệt kê các thông tin về tiến trình đã chạy trên hệ điều hành.

A screenshot of a computer

Description automatically generated

1. Kết quả câu lệnh psscan

Qua lệnh trên, ta có thể phân tích được rằng máy đang thực hiện các tiến trình đáng quan tâm gồm vm….exe ( Các tiến trình liên quan đến ứng dụng tạo máy ảo VMware), nessusd.exe ( ứng dụng scan lỗ hổng bảo mật Nessus ), Chrome.exe (trình duyệt Chrome), …

* **Lịch sử tiến trình cmd**

Để tìm kiếm lịch sử tiến trình cmd, ta có thể sử dụng lệnh consoles để trích xuất được nội dung Comand Line đã thực hiện

A screenshot of a computer

Description automatically generated

1. Kết quả lệnh consoles

Qua lệnh trên, ta có thể xác định được là người dùng đã thực thi DumpIt.exe để lưu dữ liệu của RAW hiện tại.

* **Tìm thông tin tài khọản người dùng trên máy đối tượng.**

Để tìm thông tin tài khoản trên máy dối tượng, ta sử dụng lệnh hivelist và hashdump để trích xuất các thông tin có trong Security Account Manager data

A screenshot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

1. Thông tin user trích xuất được

Dựa trên thông tin trích xuất được, ngoài 2 user mặc định là Admin và Guest, ta có một user mới là FL

* **Xem URL truy cập gần nhất.**

Dựa vào lệnh pslist, ta biết được user đang sử dụng chrome.exe với các PID 2452,2440,1852,2192,3376,3856,3132,3660 làm trình duyệt hiện tại

A black background with white numbers

Description automatically generated

Dựa theo kĩ thuật phân tích và scan để tìm cache/history tại (<https://volatility-labs.blogspot.com/2012/09/howto-scan-for-internet-cachehistory.html> ) , ta thực hiện các bước sau :

Sử dụng plugin Yara để scan thông tin trong bộ nhớ có chứa chuỗi “Client UrlCache”, đây là dấu hiệu trình duyệt có lưu lại lịch sử Cache

A screenshot of a computer

Description automatically generated

1. Kết quả yarascan với chuỗi Client UrlCache

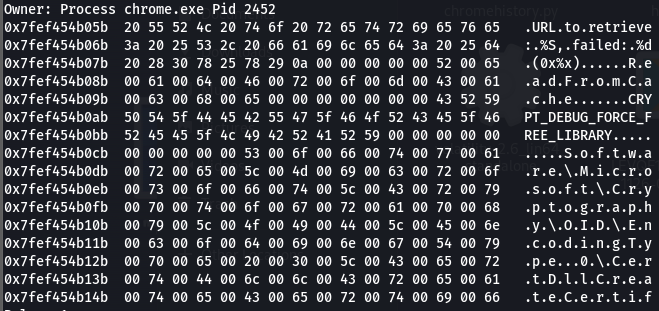
Sau khi xác định đươc có dấu hiệu trên, ta tiếp tục sử dụng yara tìm các vị trí lưu trữ có chứa chuỗi URL, đây có là đoạn cache thể chứa chuỗi URL người dùng đã truy cập. Ta tìm kiếm được một số thông tin như sau:

A screenshot of a computer screen

Description automatically generated

A screen shot of a computer screen

Description automatically generated



1. Các chuỗi URL có thể liên quan đến URL người dùng đã truy cập

---

***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)