BÁO CÁO THỰC HÀNH

**Môn học: Pháp chứng kỹ thuật số**

**Kỳ báo cáo: Buổi 06 (Session 06)**

**Tên chủ đề: CTF Final Test**

*GVHD: Đoàn Minh Trung*

*Ngày báo cáo: 29/05/2024*

**Nhóm: 07**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT334.O21.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Tấn Phát | 21522447 | 21522447@gm.uit.edu.vn |
| 2 | Nguyễn Đình Bảo Long | 21522303 | 21522303@gm.uit.edu.vn |
| 3 | Đào Vĩnh Thịnh | 21522632 | 21522632@gm.uit.edu.vn |
| 4 | Ngô Minh Thiên | 21522623 | 21522623@gm.uit.edu.vn |

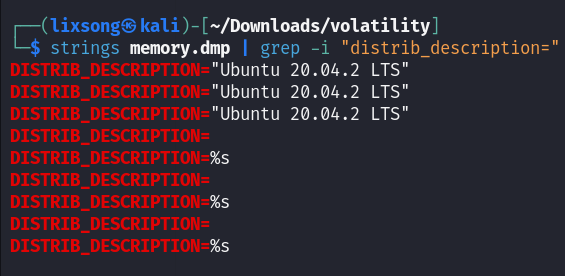
1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Thực hiện** | **Kết quả tự đánh giá** |
| 1 | Memory | Memory.dmp  Dump.raw | 100% |
| 2 | Network | Tìm IP của web server: Hoàn thành  Tìm username và password của một tài khoản sử dụng server: Hoàn thành  Hacker tấn công từ đâu: Hoàn thành  Tìm lỗ hổng hacker khai thác: Hoàn thành  Tìm tài khoản hacker đã login: Hoàn thành  Tìm Server hacker dùng để test: Hoàn thành  Tìm mật khẩu của admin: Hoàn thành  Có nên tình nghi đặc vụ đó là người đã thực hiện cuộc tấn công không? Tại sao? Hoàn thành | 100% |
| 3 | Android | Bypass\_login | 100% |
| 4 | Steganography | DecaovsDatg | 0% |

BÁO CÁO CHI TIẾT

## Memory

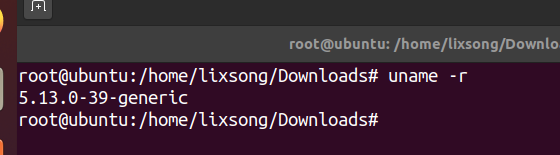
Câu Memory.dmp



Kiểm tra linux version.

A black background with white lines

Description automatically generatedThực hiện cài đặt Ubuntu20.04.01 rồi cài đặt linux-mage-5.13.0.39-generic lên đó và sử dụng



Cài đặt thêm các gói cần thiết

sudo apt install dwarfdump build-essential libelf-dev zip

Clone repo Volatility

git clone <https://github.com/volatilityfoundation/volatility.git>

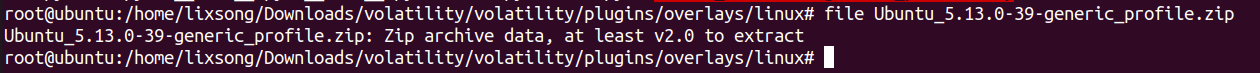
Generate the profile

cd volatility/tools/linux

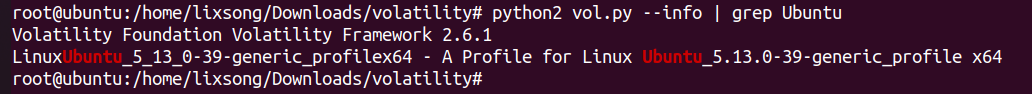
make

Zip lại tất cả mọi thứ

sudo zip $(lsb\_release -i -s)\_$(uname -r)\_profile.zip module.dwarf /boot/System.map-$(uname -r)

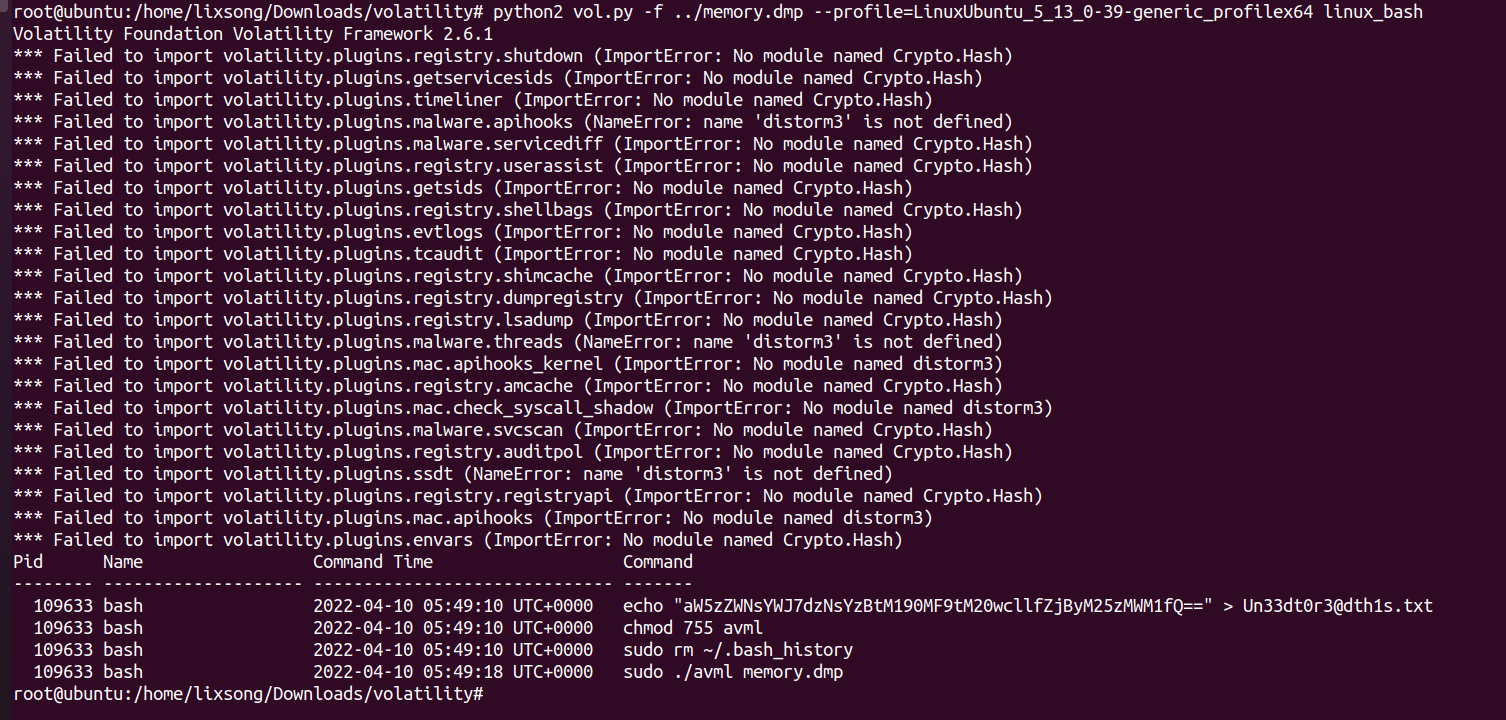


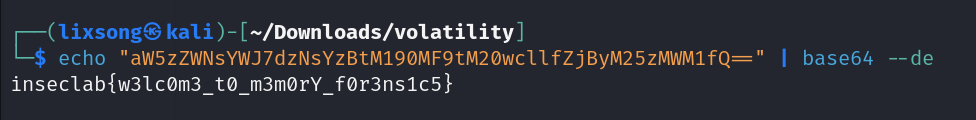
python2 vol.py --info | grep Ubuntu



Vì đề hint là linux\_bash nên ta dùng câu lệnh này để check linux\_bash

python2 vol.py -f ../memory.dmp --profile=LinuxUbuntu\_5\_13\_0-39-generic\_profilex64 linux\_bash

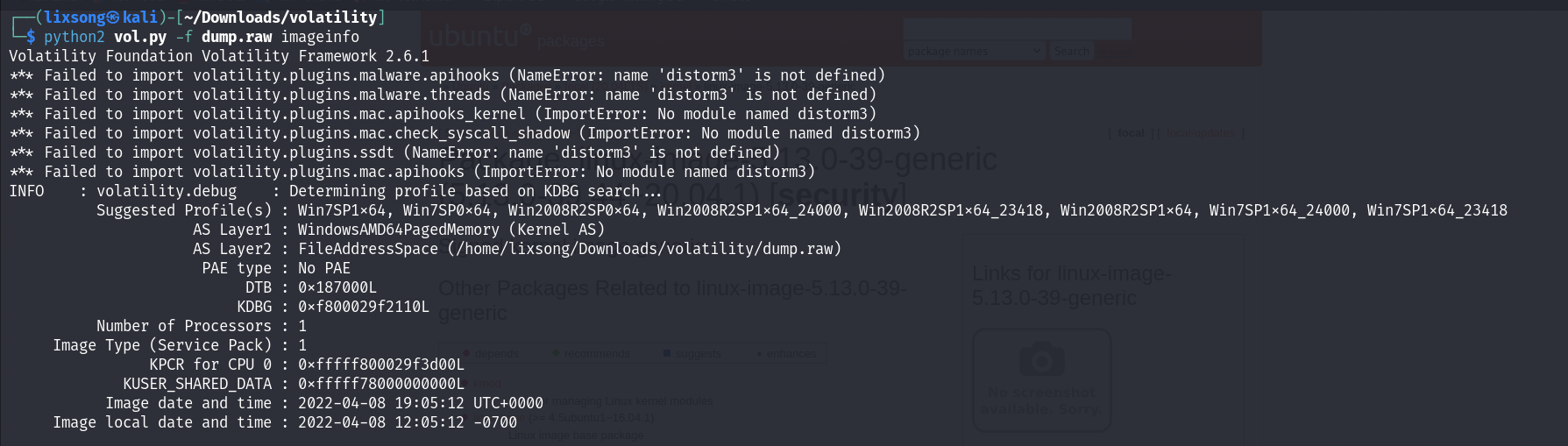


Decode đoạn base64 này  


Flag: inseclab{w3lc0m3\_t0\_m3m0rY\_f0r3ns1c5}

Câu Dump.raw

Dùng Volatility check profile của dump.raw

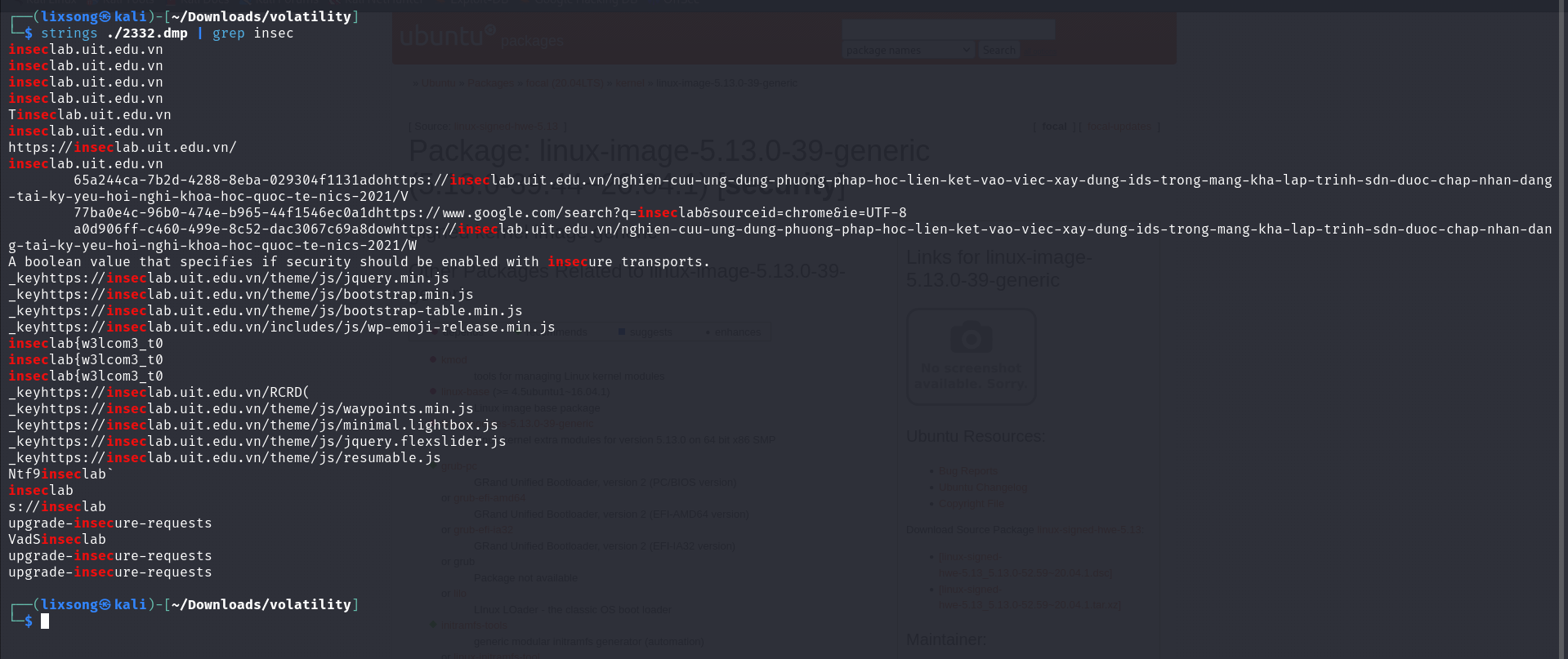


Dùng option pslist để xem thử các tiến trình

A screenshot of a computer

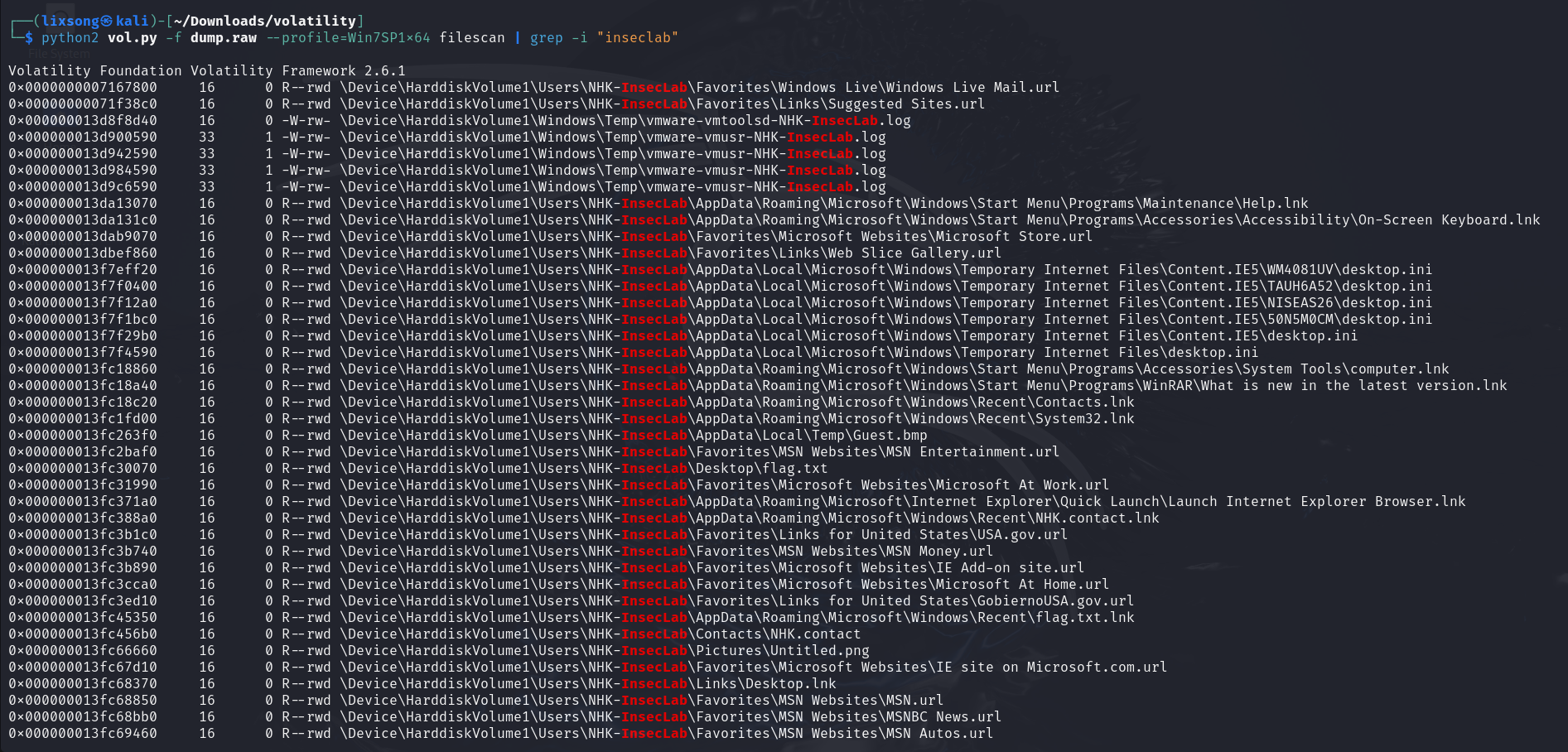
Description automatically generated

Ta dump thử tiến trình explorer.exe và chrome.exe để phân tích

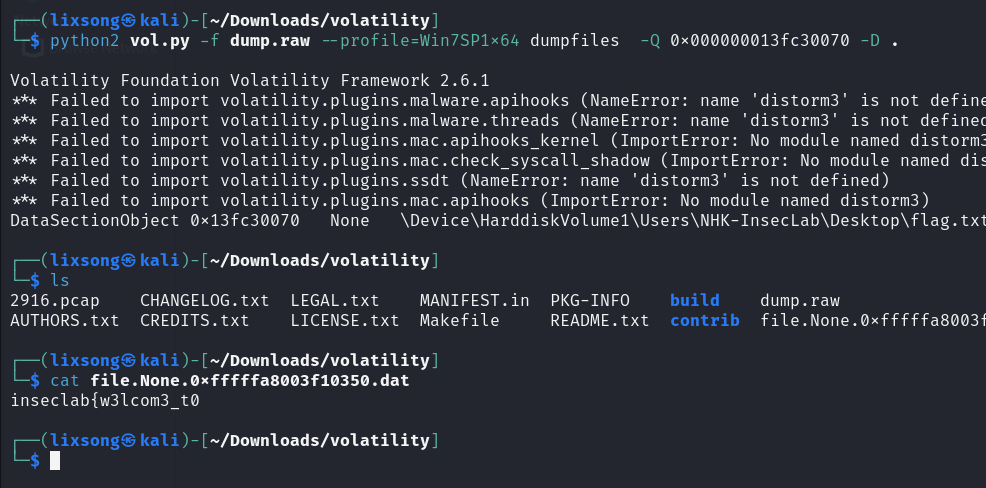
  


Tìm được 1 phần của flag: inseclab{w3lcom3\_t0

Tiếp tục dùng options filescan để tìm thông tin về inseclab

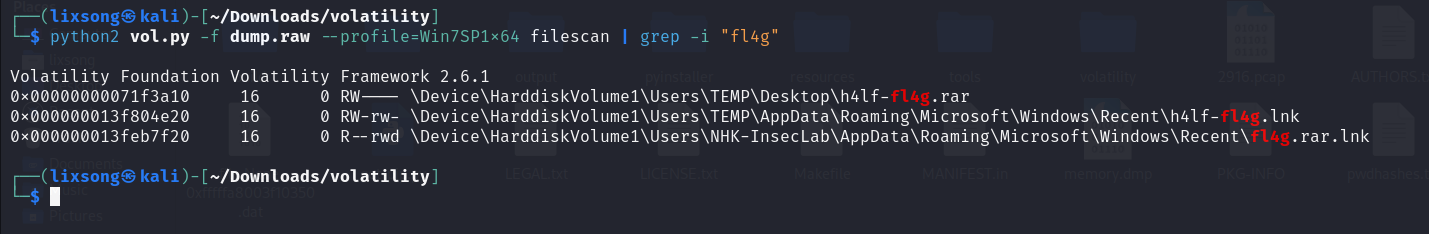


Ta thấy có file flag.txt thử dumpfiles và cat flag.txt thử nhưng vẫn ra phần đầu của flag

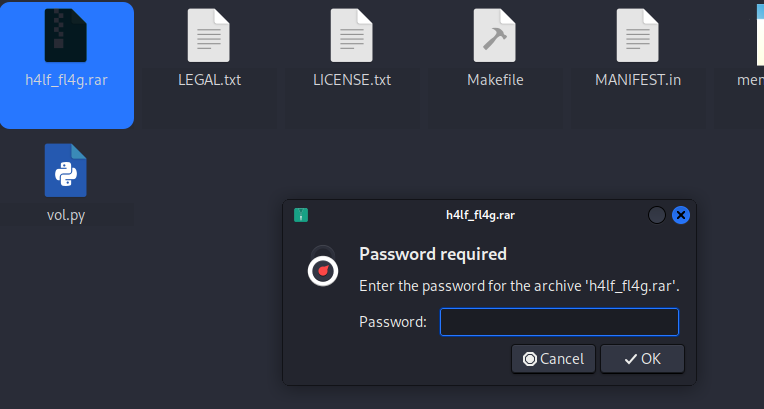


Check lại trong scan thì thấy có từ fl4g nên grep thử fl4g



Ta tìm được file h4lf-fl4g.rar  


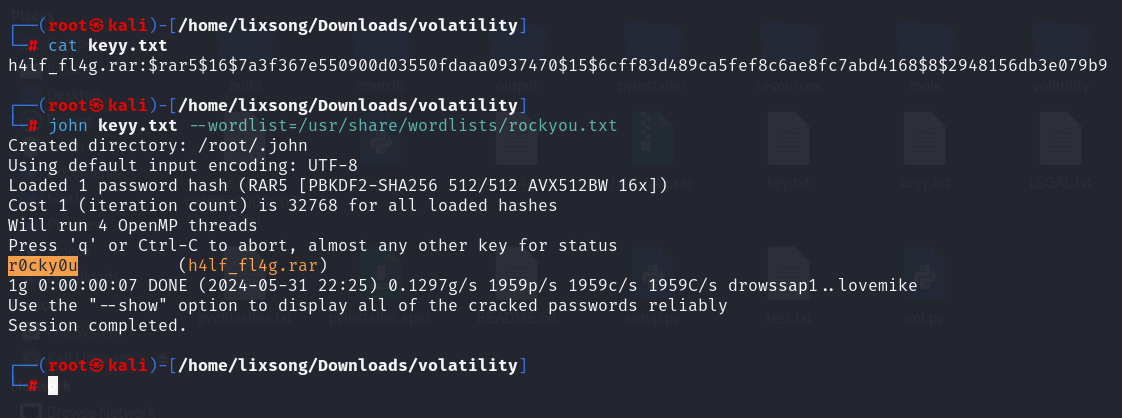
Dumpfiles này ra và extract ra nhưng thấy nó có password



Dùng tool rar2john online với đầu vào và file h4lf\_fl4g.rar và đưa vào file key.txt

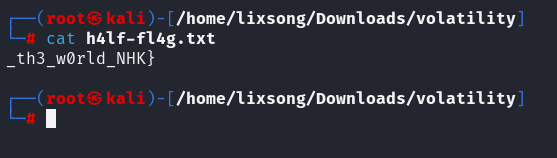
A screenshot of a computer

Description automatically generated



Dùng tool john với wordlists rockyou.txt để crack password

Password tìm được là r0cky0u. Dùng password này để extract file h4lg\_fl4g.rar ta thu được nửa còn lại của flag.

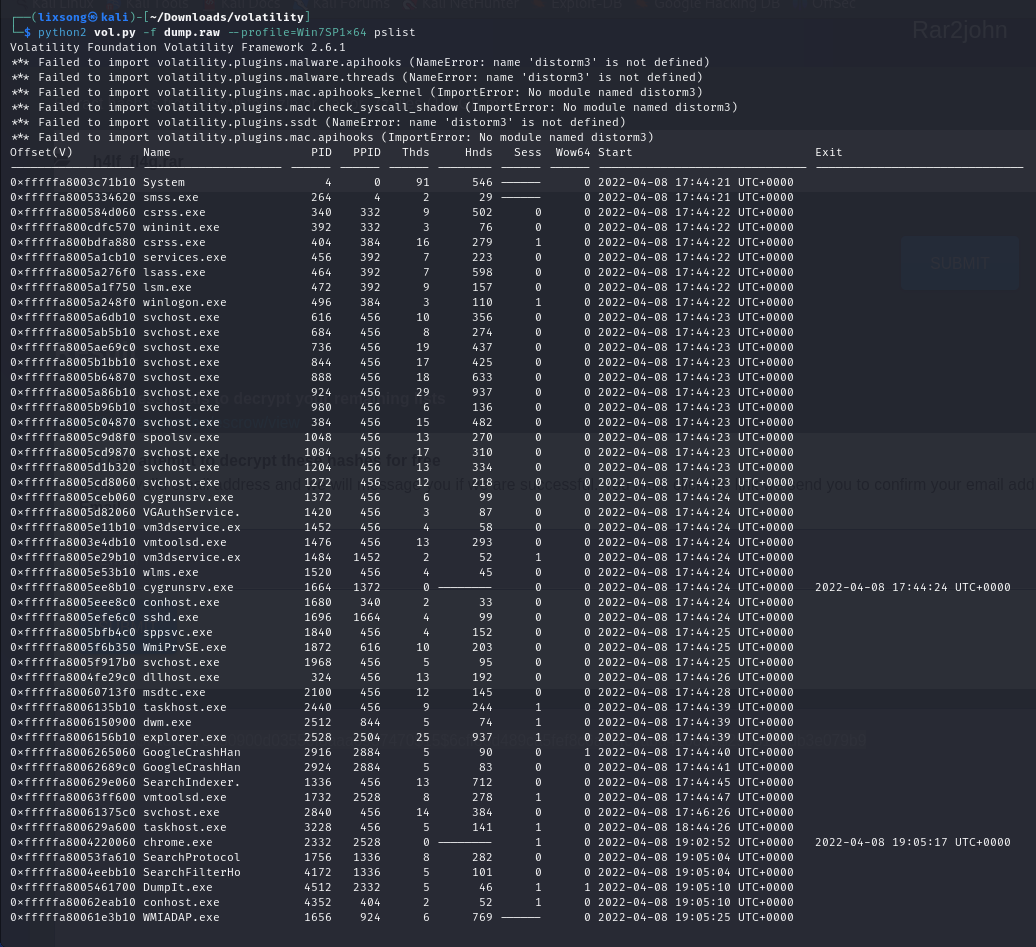


Flag hoàn chỉnh là: inseclab{w3lcom3\_t0\_th3\_w0rld\_NHK}

Yêu cầu 2: Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra: + Liệu họ có để lại những dấu vết trên trình duyệt web?.

Đầu tiên, dùng plugins pslist để xem các process mà máy nạn nhân đang sử dụng để tìm các trình duyệt sử dụng

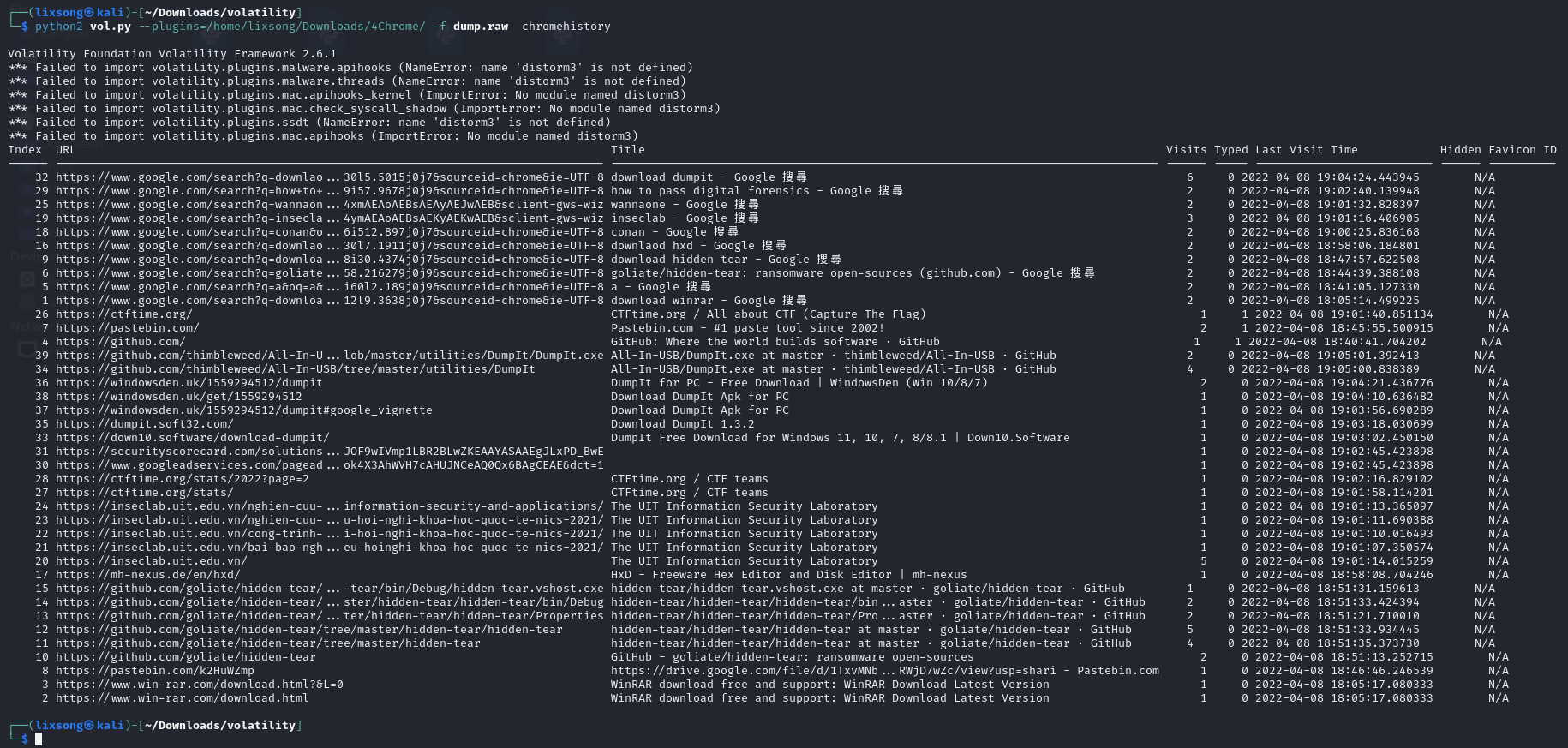
python2 vol.py -f dump.raw --profile=Win7SP1x64 pslist



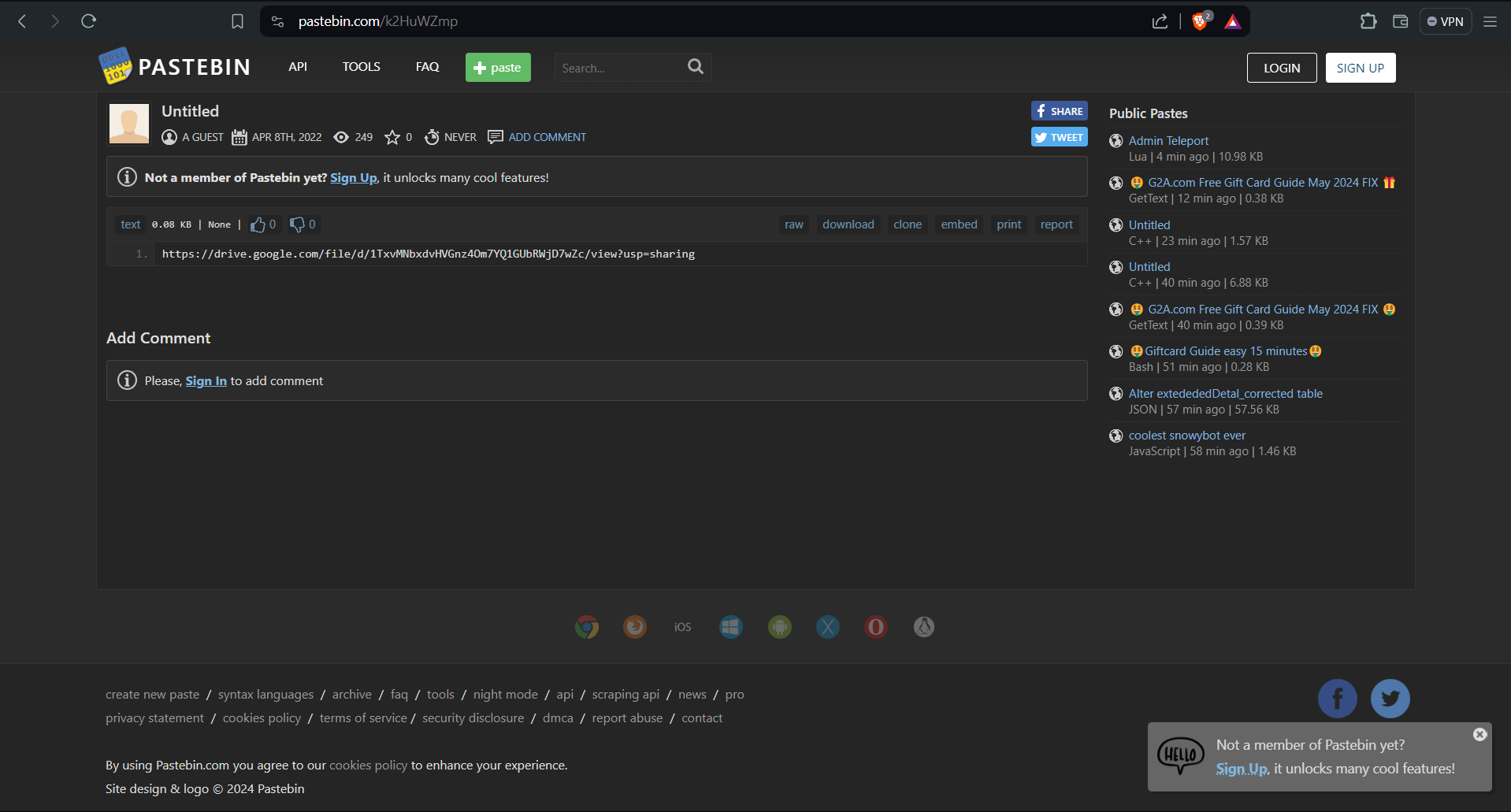
Ta thấy có sử dụng chrome, internet explorer. Ta thử kiểm tra chrome.

Ở đây ta cài thêm 2 file chromehistory.py và sqlite\_help.py để chạy được plugin chromehistory

python2 vol.py --plugins=/home/lixsong/Downloads/4Chrome/ -f dump.raw chromehistory



Ta phân tích thì thấy user này có vào 1 trang pastebin - pastebin là một trang giúp cho mọi người lưu trữ và chia sẽ text. Thử đi vào đường dẫn này thử thì thấy có dẫn đến một link google drive.



Ta vô trang drive

A screenshot of a computer

Description automatically generated

Thấy bảo là nothing here,but in here ta thử bôi đen thì thấy file còn kéo dài   
A screenshot of a computer

Description automatically generated

* Tải về và dùng xxd xem thử

A screen shot of a computer

Description automatically generated

Sau khi tìm hiểu thì tìm tool stegsnow để giải mã.

A computer screen shot of a code

Description automatically generated

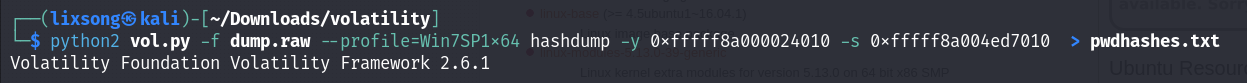
Flag: inseclab{y0u\_c4n\_s33\_fl4g}

Yêu cầu 3: Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra: Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password laptop của NHK. Hãy tìm password đó.

Thử nghiệm lấy thông tin mật khẩu.

Ở đây ta dùng hivelist để lấy ra trường địa chỉ bắt đầu trọng bộ nhớ của nơi lưu trữ thông tin đăng ký và quản lý về tài khọản người dùng Windows.A screen shot of a computer

Description automatically generated

Sau đó ta trích xuất mã băm mật khẩu vào một tập tin text để tiện quan sát

Mật khẩu đã được hash và thông tin chỉ được lưu lại ở dạng hash.

A screen shot of a computer

Description automatically generated

Đã thử dùng hashcat và tool hashes online nhưng ko ra kết quả pass ở dạng plaintext.

Thử dùng plugins lsadump để xem pass nhưng ko có



Tải và cài đặt plugins mimikatz để tìm password

A screen shot of a computer

Description automatically generated

Flag: inseclab{AntiNHK}

## Network

1. Tìm IP của web server.

Sử dụng Statistics cho Ipv4 thì ta thấy tổng số packet của IP 224.0.0.251 và 172.18.0.3 bằng 122213, tổng số packet của 3 IP còn lại cũng bằng 122213

A screenshot of a computer

Description automatically generated

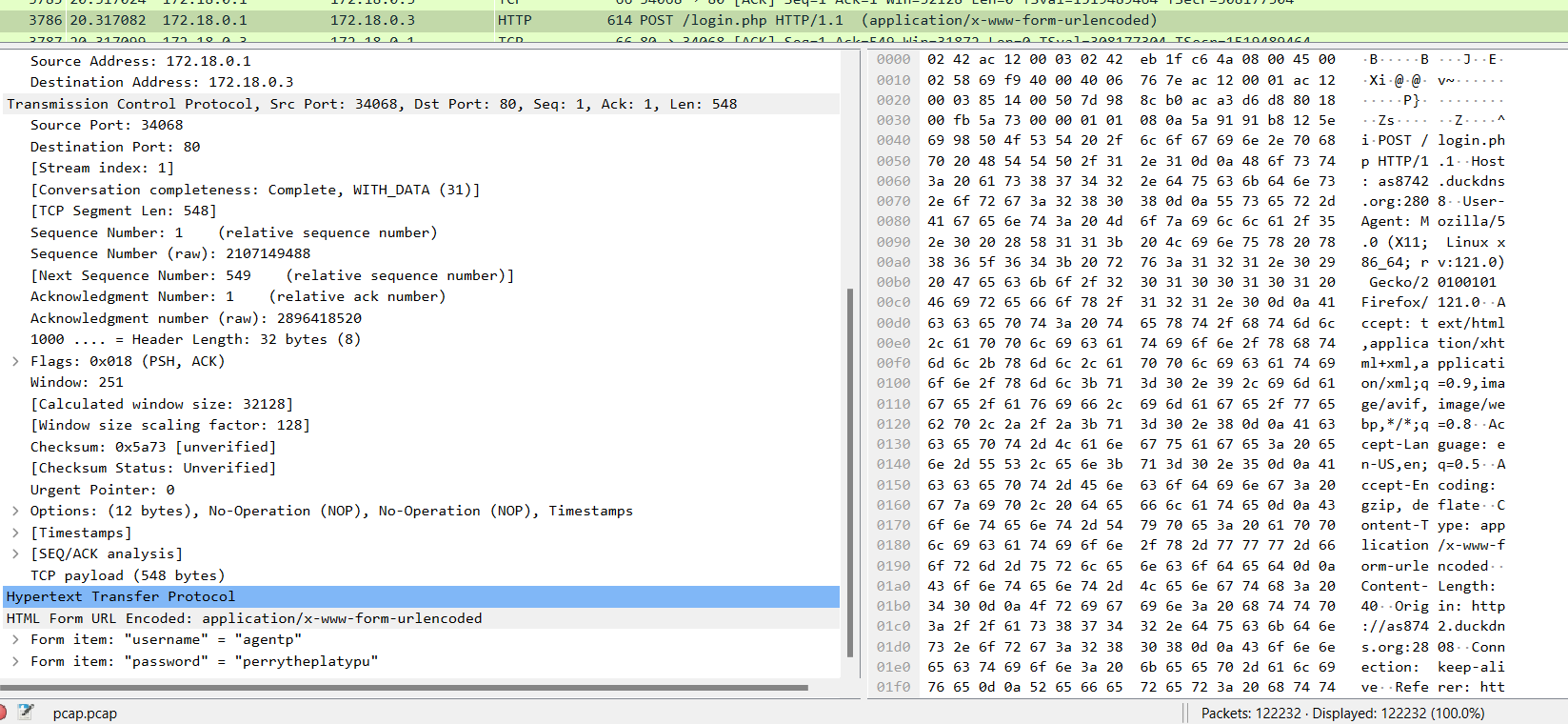
Xem qua vài packet thì thấy đa số là IP 172.18.0.3 response, 172.18.0.2 thì response các gói tin qua giao thức MySQL nên có thể đây là database của server, 172.18.0.1 có thể là default gateway. Vậy mô hình mạng theo em suy đoán thì hacker sử dụng máy có IP 151.101.78.132. IP của server là 172.18.0.3

A close-up of a computer screen

Description automatically generated

1. Tìm username và password của một tài khoản sử dụng server. NHK nghe nói anh ta là một đặc vụ mật.

Sử dụng Ctrl+F tìm string “login”, gói tin 3786 có hiện thông tin username là ‘agentp’ và password là "perrytheplatypu"



1. Hacker tấn công từ bên ngoài mạng hay là từ bên trong mạng.

Theo câu a thì hacker tấn công từ bên ngoài mạng

1. Lỗ hổng là hacker dùng để khai thác là gì?

Trong file pcap có rất nhiều packet có payload giống như sau, vậy nên attacker khai thác lỗ hổng SQL injection

1. Hacker đã login vào tài khoản nào?

Ở packet 4929 ta lại thấy POST request gửi tới server với cùng username và password nhưng lần này password có thêm chữ ‘s’ thay vì bị thiếu như packet trước

A screen shot of a computer

Description automatically generated

Packet 7073 cũng có 1 POST request gửi với username và password là admin

A screenshot of a computer

Description automatically generated

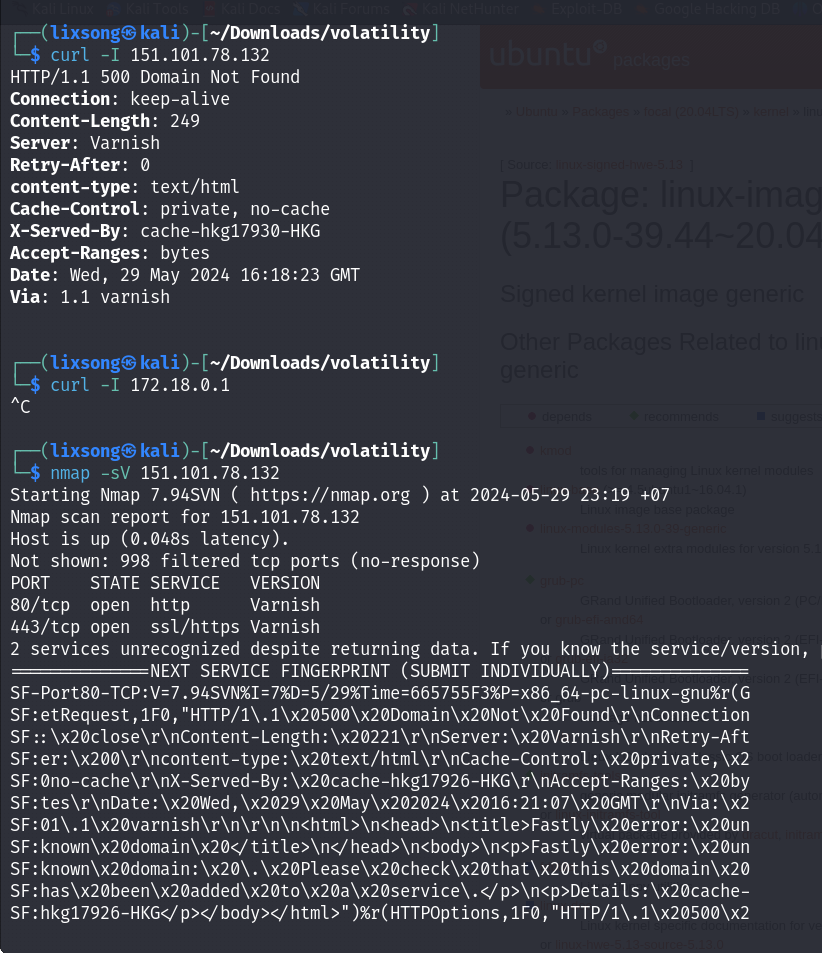
1. Server mà hacker dùng để test là gì?

Ở đây server hacker dùng dể test là MySQL Database server

A screenshot of a computer

Description automatically generated

Như câu a thì ta đoán IP của hacker là 151.101.78.132 nên ta có thể thử dùng curl và nmap để thử xác định server của hacker



Có thể thấy service ở đây là Varnish.

Theo tìm hiểu thì Varnish hoạt động như một reverse proxy, đứng giữa người dùng và server backend. Các yêu cầu từ người dùng sẽ được gửi tới Varnish trước, sau đó Varnish sẽ quyết định có nên trả về nội dung từ cache hay chuyển tiếp yêu cầu tới server backend.

Do vậy hacker đã dùng Varnish để che giấu đi server của hacker thật sự nên chưa thể tìm ra…..

1. Có vẻ là hacker đã lấy được mật khẩu của admin. Nhưng có người lại bảo là chưa. Vậy hacker đã lấy được mật khẩu của admin chưa? Mật khẩu của admin là gì? Hacker đã lấy được gì?

Từ khoảng packet thứ 87000 trở đi em thấy có rất nhiều packet có payload như sau

A screenshot of a computer

Description automatically generated

Thử dùng chatgpt với promt “convert this payload to readable string for me” để hiểu payload dùng để làm gì

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

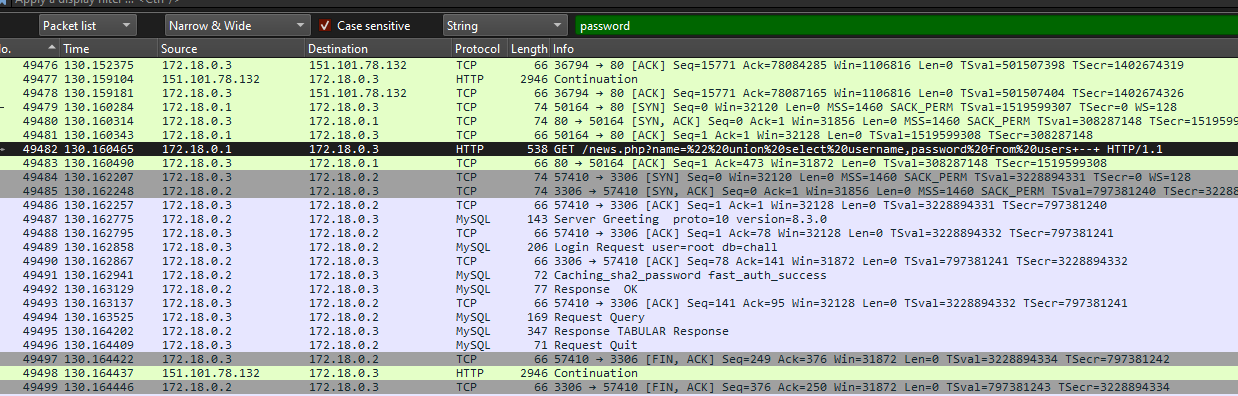
Chatgpt còn giải thích giúp thêm về payload, thì em hiểu payload sẽ so sánh kí tự đầu tiên của password cho user ‘admin’ có phải là ‘@’ hay không, nếu đúng thì sẽ sleep 4s. Lúc này em sẽ đi tìm những khoảng thời gian hacker gửi payload tấn công tới server và bị ngắt khoảng 4s không gửi payload tấn công nữa.

A screen shot of a computer

Description automatically generated

Em tìm được rất nhiều packet như trên và sử dụng chatgpt để chuyển đổi payload thành dạng dễ đọc hơn. Sau đó em ghép các kí tự lại với nhau thì được chuỗi “@dm1n\_3r37\_!@#~” nhưng bị thiếu kí tự thứ 7 và 9.

Lúc này em đi search lại string ‘password’ ở các packet injection đầu tiên xem có bỏ sót gì không thì gặp packet 49482, packet này rất khác các packet trên, em xem thử các packet response thì packet 49495 trả về tabular



Mở ra xem thử thì có toàn bộ username và password luôn

A screenshot of a computer program

Description automatically generated

Vậy hacker đã lấy được mật khẩu admin là “@dm1n\_s3cr37\_!@#”

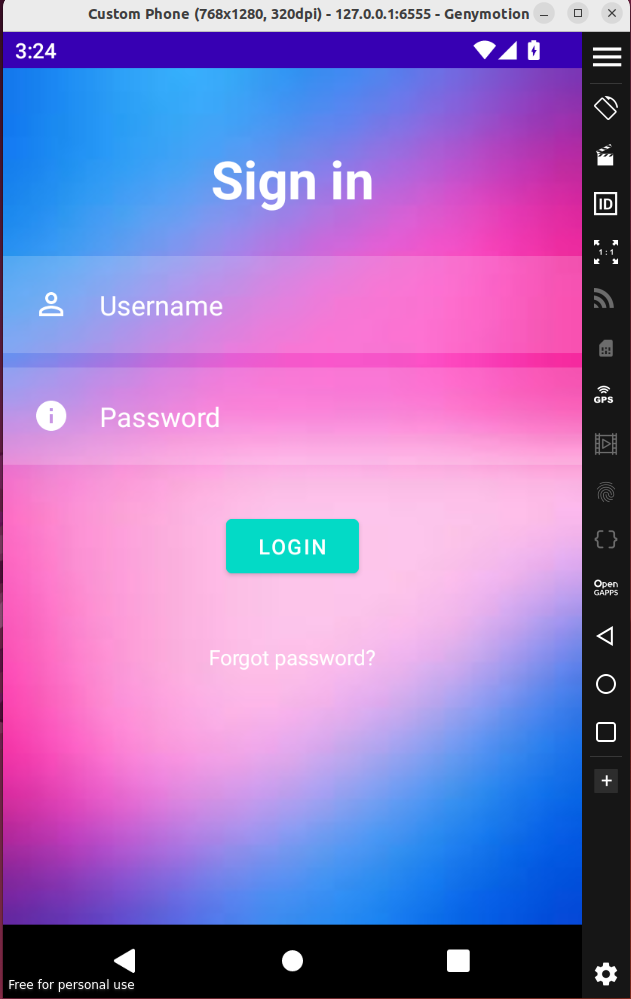
1. Có nên tình nghi đặc vụ đó là người đã thực hiện cuộc tấn công không? Tại sao?

Theo em thì hacker không phải Agent P, hacker không biết pass admin nên không phải là người get TABULAR ở packet 49495, nếu đã biết account thì không cần attack, thêm 1 tí bằng chứng ngoài lề là Agent P là đặc vụ giữ an toàn cho khu vực Tri-State Area nên khá chắc đặc vụ không làm việc này.

## Android

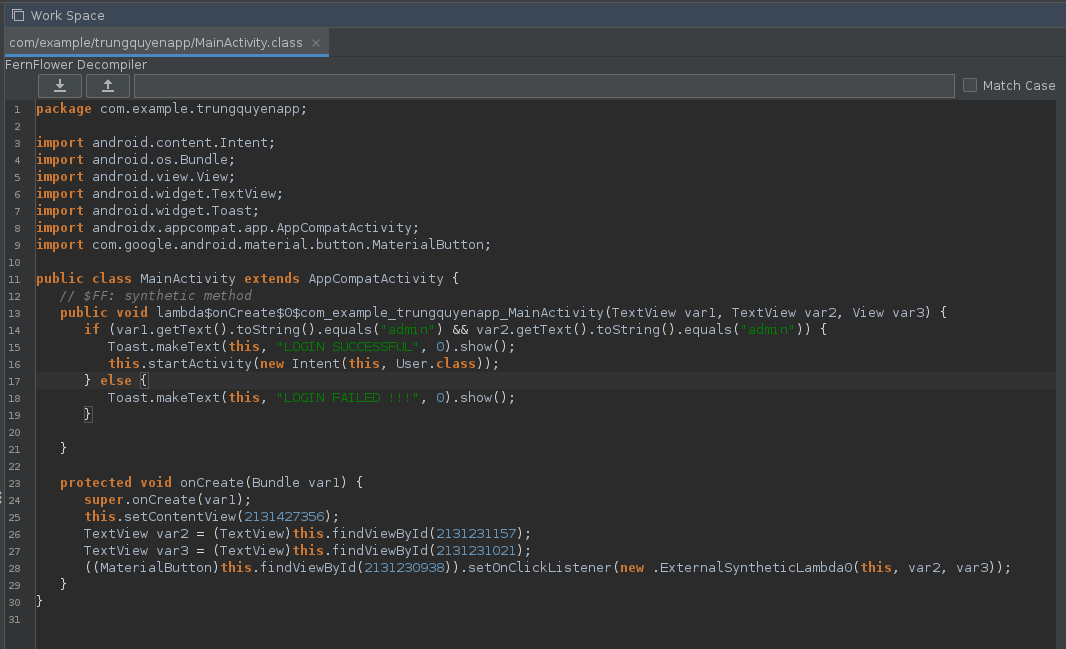
Mở app thấy giao diện như này

Có vẻ yêu cầu ta Login thành công sẽ có flag



Dùng ByteCode-Viewer để đọc code.

Đọc và phân tích code hàm MainActivity



Ta thấy username và password là admin thì login thành công.



Ta có được flag: inseclab{w3lc0m3\_t0\_@ndr01d\_Ch@ll3ng3!!!}

Đoạn mã bạn cung cấp chứa một số lỗi bảo mật nghiêm trọng liên quan đến việc xử lý thông tin đăng nhập và bảo vệ thông tin nhạy cảm. Dưới đây là phân tích về các lỗi và biện pháp khắc phục:

Lỗi bảo mật

1. Thông tin đăng nhập cứng (Hard-coded credentials):

- Thông tin đăng nhập `admin` được mã hóa cứng trong mã nguồn. Điều này có nghĩa là bất kỳ ai có quyền truy cập vào mã nguồn đều có thể dễ dàng nhìn thấy thông tin đăng nhập này.



2. So sánh chuỗi không an toàn:

- So sánh chuỗi sử dụng phương thức `equals` mà không có biện pháp bảo vệ trước các tấn công thời gian (timing attacks).

- Điều này có thể bị lợi dụng để đoán mật khẩu dựa trên thời gian phản hồi của ứng dụng.

Biện pháp khắc phục

1. Loại bỏ thông tin đăng nhập cứng:

- Không bao giờ lưu trữ thông tin đăng nhập hoặc thông tin nhạy cảm trực tiếp trong mã nguồn. Thay vào đó, sử dụng cơ sở dữ liệu hoặc các dịch vụ xác thực bên ngoài.

- Sử dụng các phương pháp xác thực an toàn như OAuth, JWT, hoặc các phương pháp xác thực hai yếu tố (2FA).

2. Sử dụng các hàm băm và mã hóa an toàn:

- Mật khẩu nên được lưu trữ dưới dạng băm (hash) với một salt ngẫu nhiên và sử dụng các thuật toán băm mạnh như bcrypt, Argon2, hoặc PBKDF2.

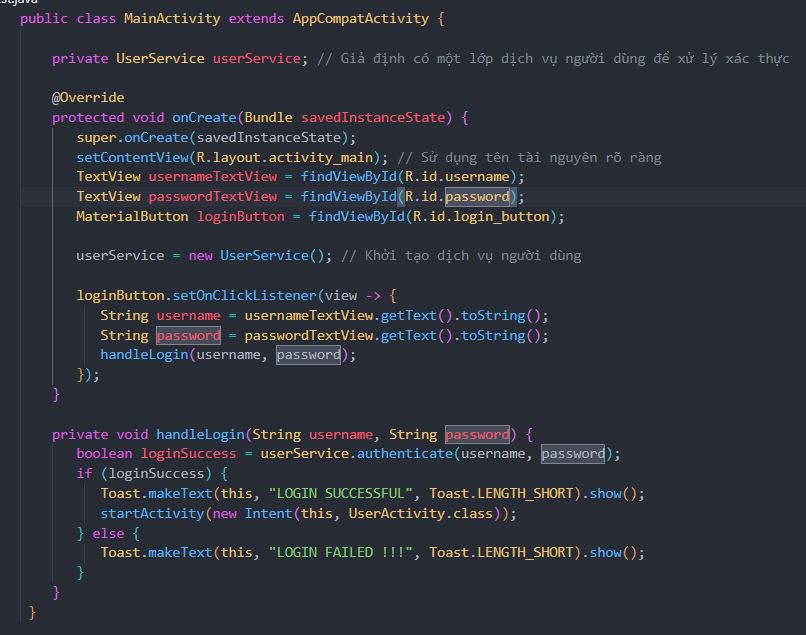
- Khi người dùng đăng nhập, so sánh mật khẩu đã băm của họ với mật khẩu đã băm được lưu trữ.

3. Sử dụng biện pháp bảo vệ trước các tấn công thời gian:

- Sử dụng các thư viện bảo mật đã được kiểm chứng để so sánh các chuỗi an toàn, như thư viện `MessageDigest` hoặc `SecretKeySpec` trong Java.

Đề xuất mã sửa đổi

Dưới đây là một ví dụ về cách cải thiện đoạn mã đăng nhập:



Tóm tắt

- Loại bỏ thông tin đăng nhập cứng khỏi mã nguồn.

- Sử dụng cơ sở dữ liệu để lưu trữ thông tin người dùng và mật khẩu đã băm.

- Sử dụng các thư viện băm mạnh và so sánh chuỗi an toàn.

- Triển khai các biện pháp bảo mật như xác thực hai yếu tố (2FA) để tăng cường bảo mật.

## Steganography

---

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

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo 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]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

*Ví dụ: [NT101.H11.1]-Session1\_Group3.*

* 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 Lab.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

* Chuẩn bị tốt và đóng góp tích cực tại lớp.
* Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*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)