BÁO CÁO BÀI TẬP

**Môn học: Bảo mật Web và Ứng dụng**

**Kỳ báo cáo: Buổi 03 (Session 03)**

**Tên chủ đề: Recon**

*GV: Nghi Hoàng Khoa*

*Ngày báo cáo: 12/04/2023*

**Nhóm: XX (nếu không có xoá phần này)**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT101.N21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Võ Anh Kiệt | 20520605 | 20520605@gm.uit.edu.vn |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | 7 Kịch bản | 100% |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

BÁO CÁO CHI TIẾT

## Kịch bản 01

Ở câu 1 ta sẽ sử dụng virustotal.com để thực hiện kiểm tra các domain thì ta có thể lấy được 101 domain

https://www.virustotal.com/gui/domain/rmit.edu.vn/relations



## Kịch bản 2

Ở câu 2 ta thực hiện tấn công bằng intruder với 5000 payload ở cách 1

Graphical user interface, text, application

Description automatically generated

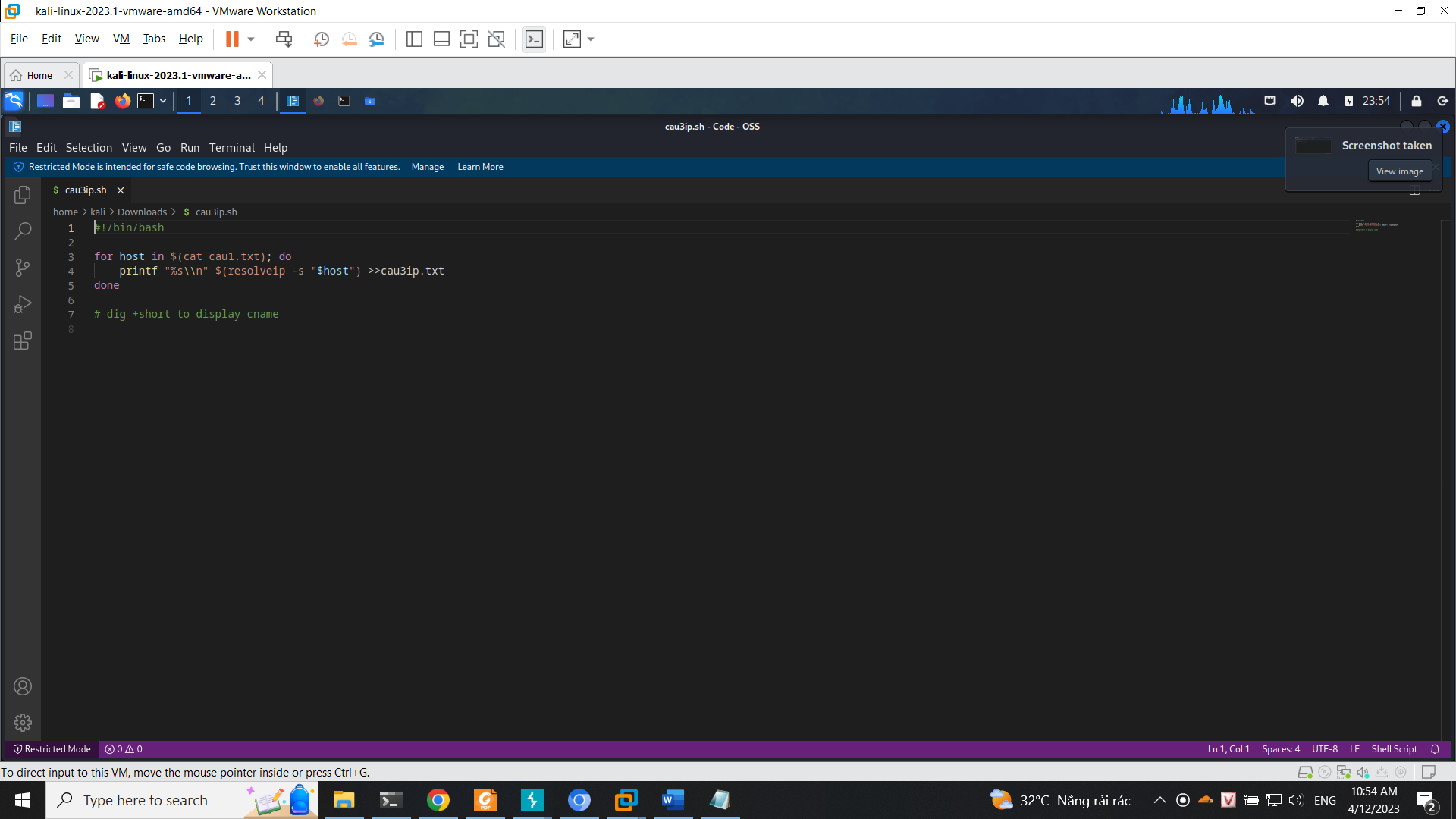
Ngoài ra ta có thể thực hiện việc tấn công bằng các payload được filter lại từ các subdomain tìm được ở câu 1 và thực hiện tấn công, ở đây ta thấy được rằng là để lọc được các thông tin như là status thì ta sẽ ấn vào trường status, điều này sẽ khiến cho việc lọc status dễ dàng hơn

Graphical user interface, text, application

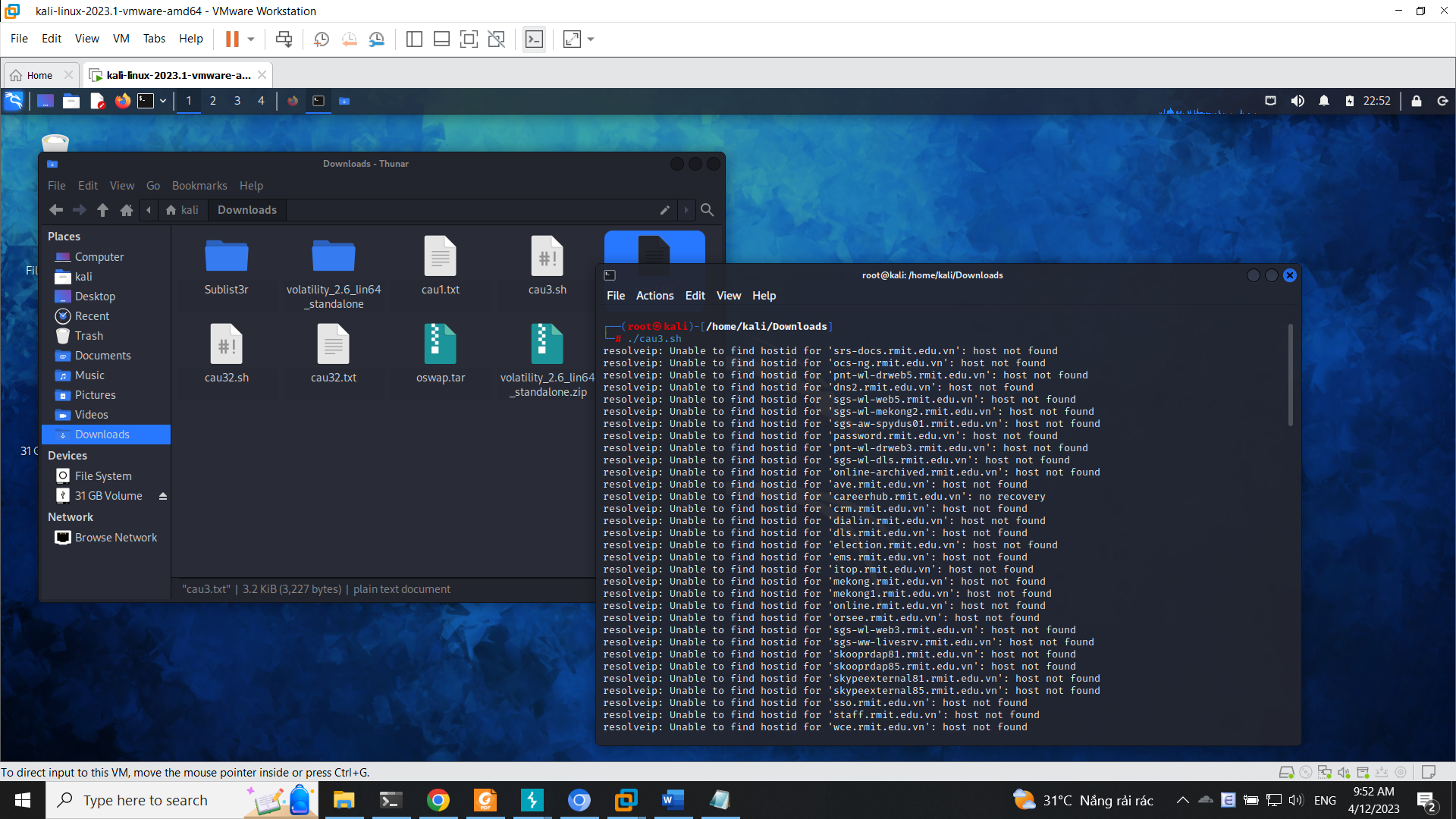
Description automatically generated

## Kịch bản 3

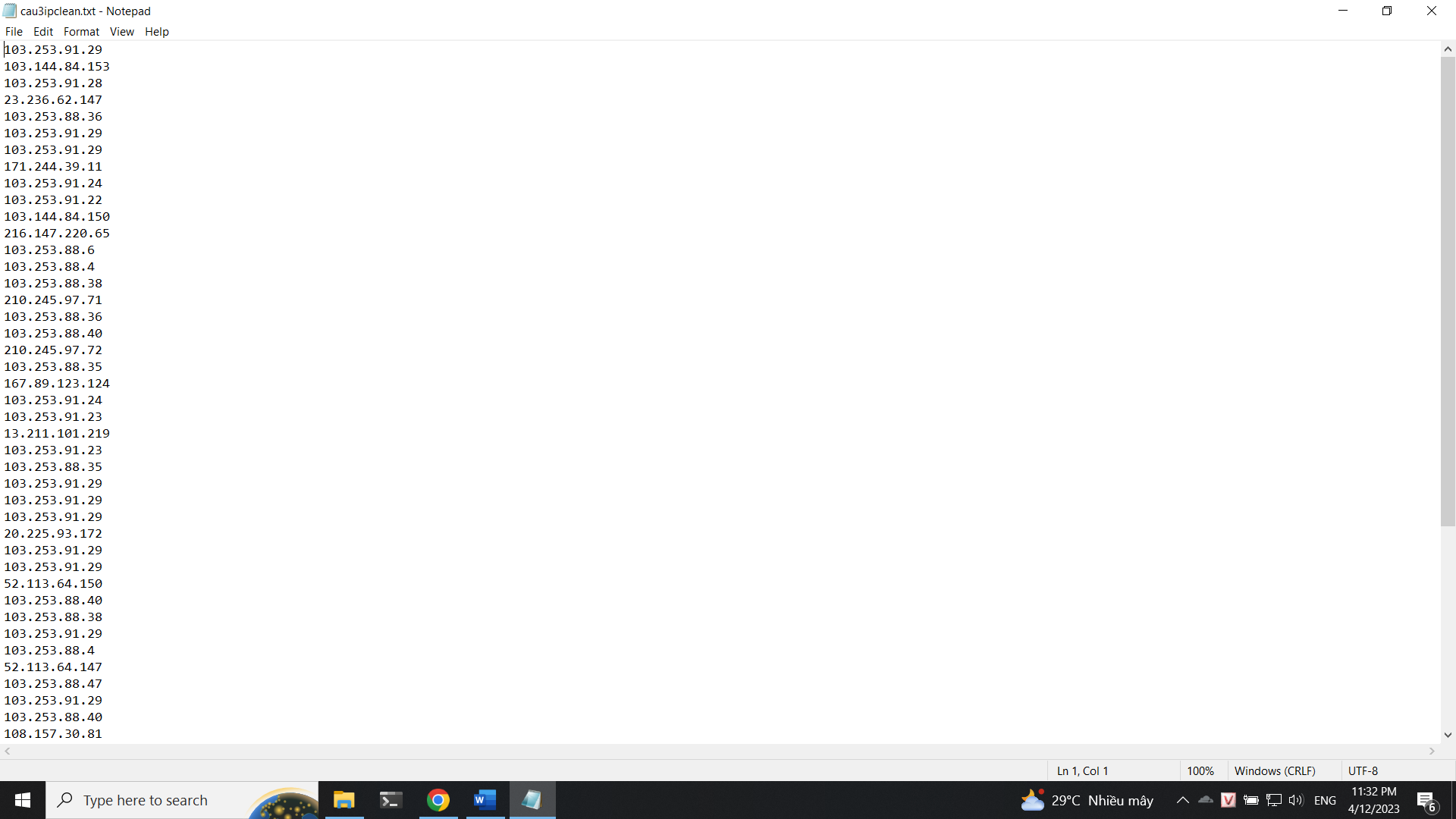
Đầu tiên ta sẽ thực hiện tạo shell như hình để có thể lấy được ip, ý nghĩa: với mỗi host trong file cau1.txt thì ta sẽ resolve ip ra từ host đó và gán vào file cau3ip



Thực thi chương trình thì ta thấy có một số tên miền không có hostid



Sau khi thực hiện xong và filter lại file thì ta có kết quả



## Kịch bản 4

Đầu tiên ta tiếp tục thực hiện việc tìm các port đang mở của từng ip, ý nghĩa code: với mỗi ip tìm được trong câu 3 thì sẽ sử dụng naabu để tìm port và gán giá trị vào cau4.txt

A screenshot of a computer

Description automatically generated

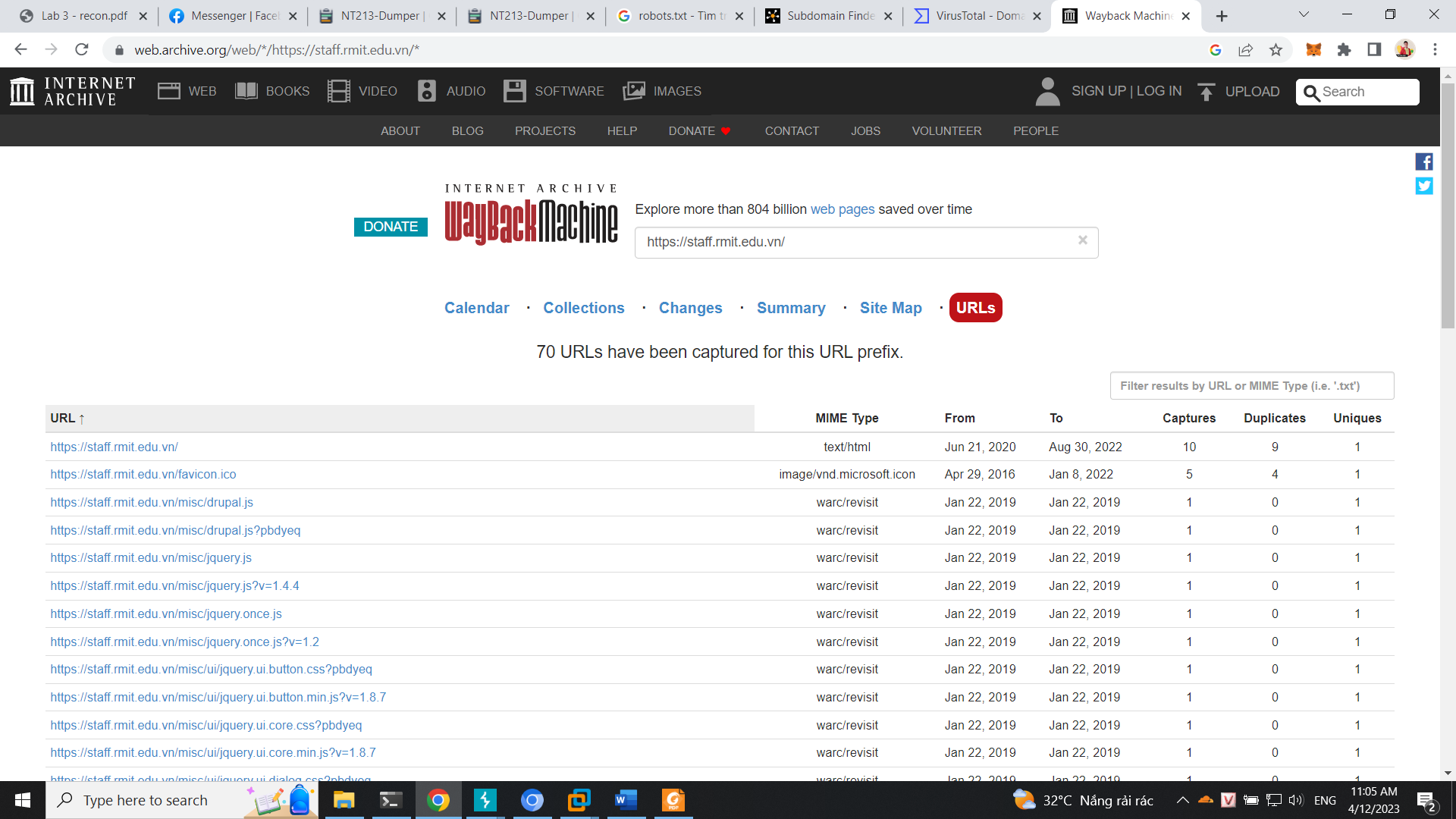
Sau khi thực hiện xong thì ta có được kết quả

A screenshot of a computer

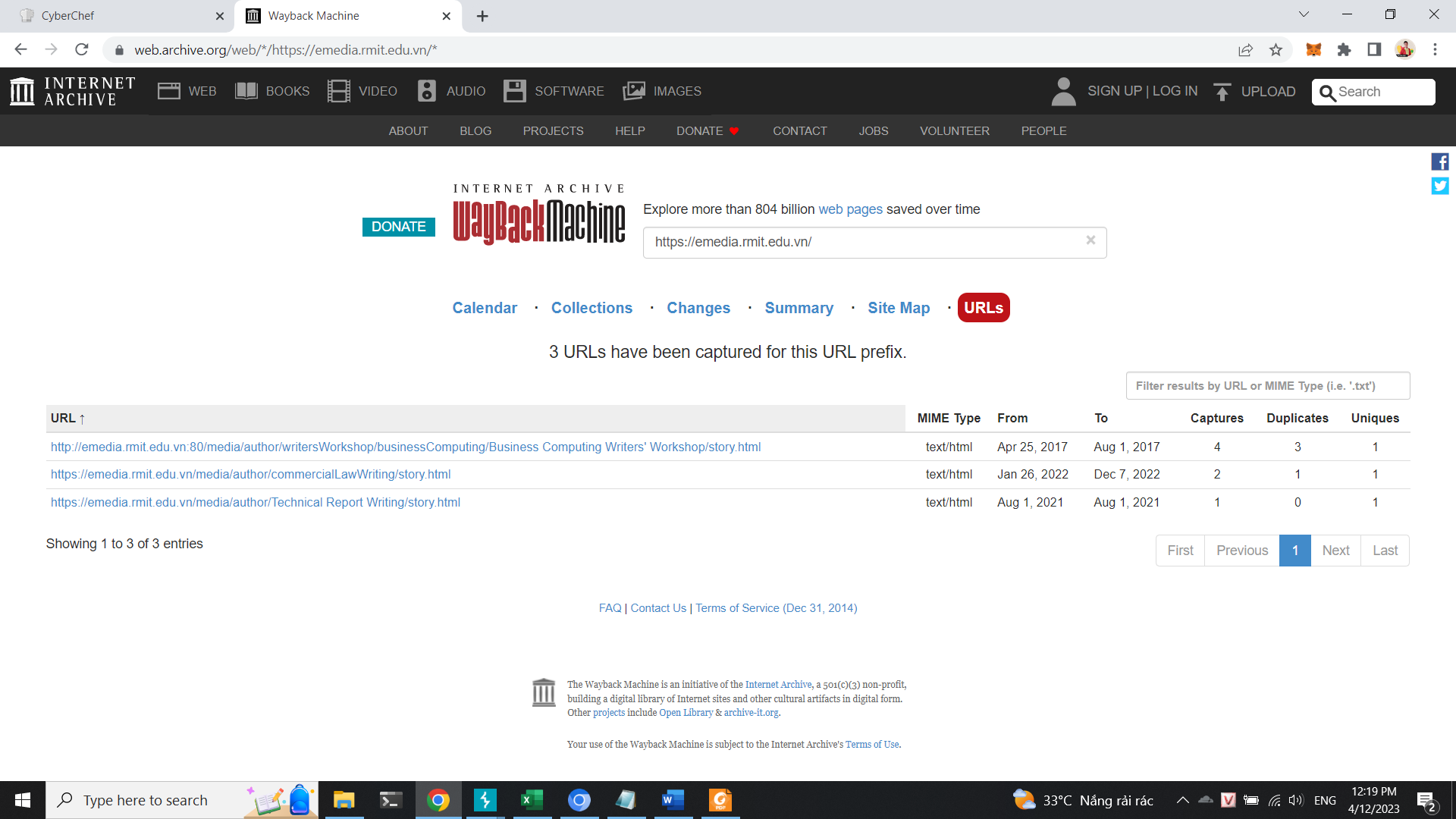
Description automatically generated

## Kịch bản 5

Ở câu 5 ta sẽ sử dụng web archive để xem những domain nào không còn hoạt động nữa thì ta thấy được trong đó domain với subdomain là staff không còn hoạt động



Thực hiện tương tự ta cũng thấy được thông tin đó chính là domain với subdomain là emedia cũng không còn hoạt động nữa



## Kịch bản 6

Ở câu 6 ta sẽ sử dụng google dork để kiểm tra xem với tên miền nào thì ta có được các filetype là tài liệu doc, pdf hay file excel dạng xls

Ở đây ta sẽ thực hiện việc vào google dork và tìm kiếm thì ta có cách tìm bên dưới và kết quả như hình

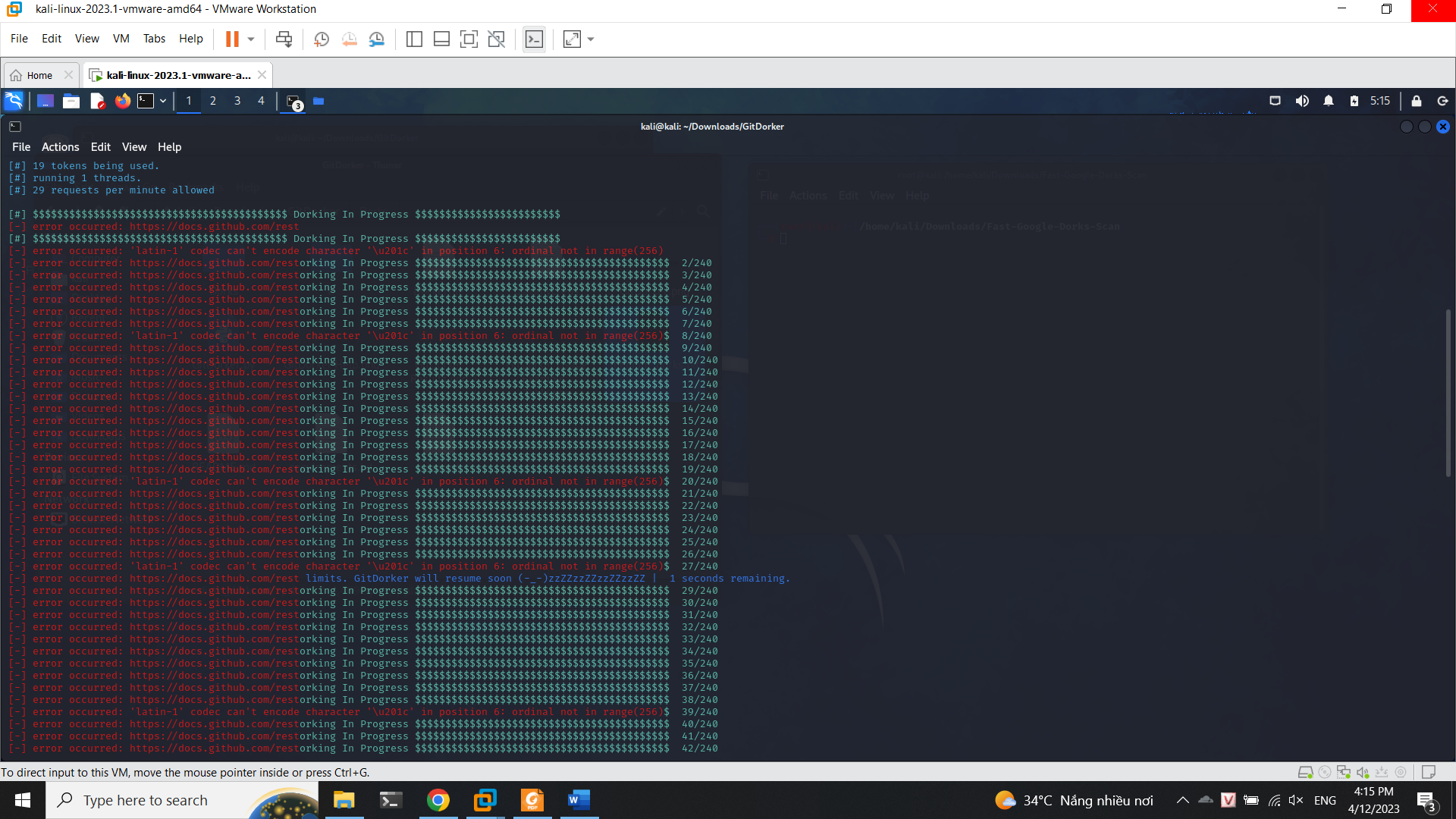
site:alumninetwork.rmit.edu.vn filetype:pdf OR filetype:doc OR filetype:xls

Graphical user interface, text, application

Description automatically generated

## Kịch bản 7

Cách 1 ta sẽ sử dụng tool để thực hiện quét

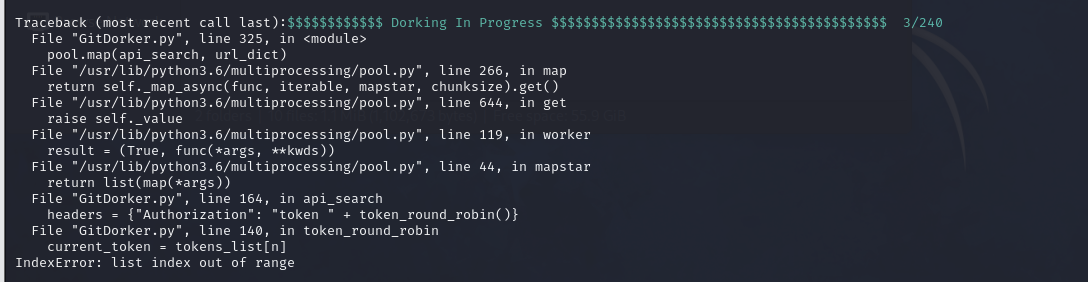


Nhưng do bị bug và chưa fix được, đã báo cáo lên nhóm

Graphical user interface, text

Description automatically generated

Bạn Nguyên cũng hướng dẫn sử dụng docker nhưng do vấn đề là khi sử dụng docker thì sẽ phát sinh lỗi mới



Ngoài ra ta có thể sử dụng phương pháp manual bằng cách vào github và gõ phần domain và token thì ta có thể xem được những thông tin nhạy cảm

Graphical user interface, text, application

Description automatically generated

---

***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 .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/Tên Cá nhân đã đăng ký với GV).

*Ví dụ: [*NT101.K11.ANTT*]-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.
* 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. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*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)