

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: 13/04/2023

Nhóm: XX (nếu không có xóa phần này)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.N21.ANTN

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

2. NỘI DUNG THỰC HIỆN:¹

| STT | Công việc | Kết quả tự đánh giá | Người đóng góp |
|-----|-------------|---------------------|----------------|
| 1 | Kịch bản 01 | 100% | |
| 2 | Kịch bản 02 | 100% | |
| 3 | Kịch bản 03 | 100% | |
| 4 | Kịch bản 04 | 100% | |
| | | | |

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

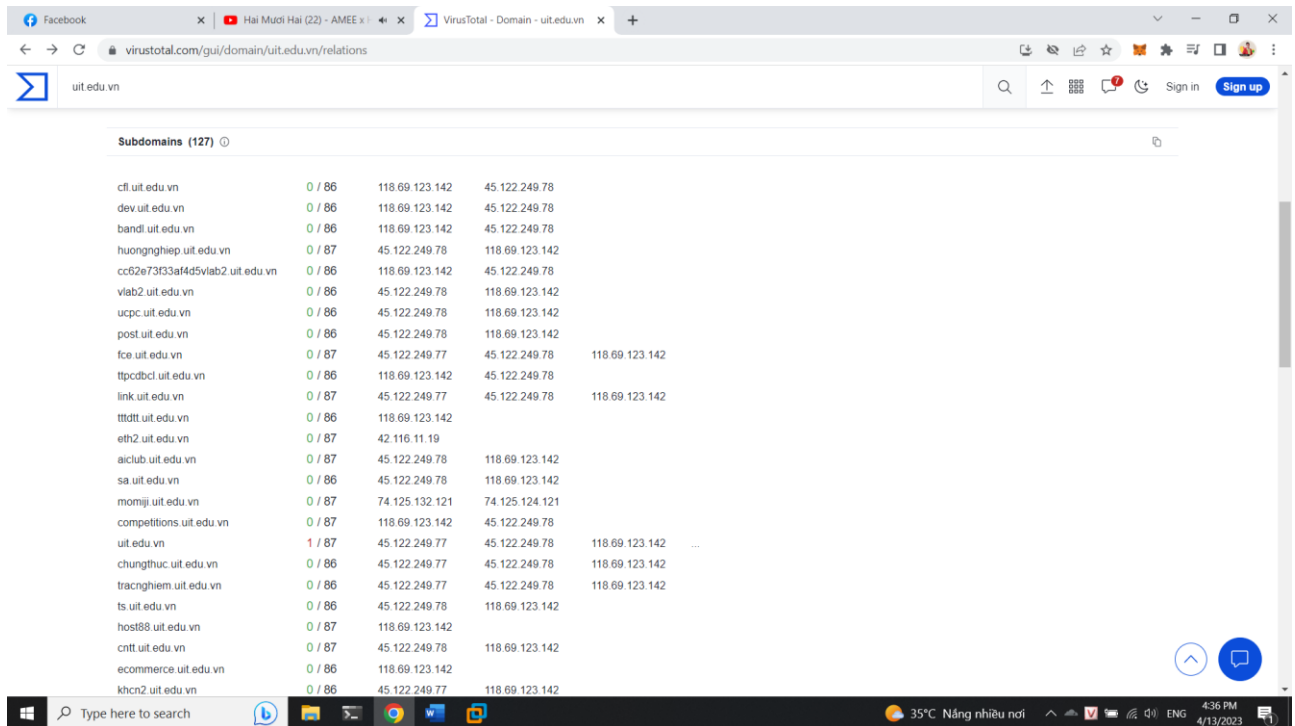
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

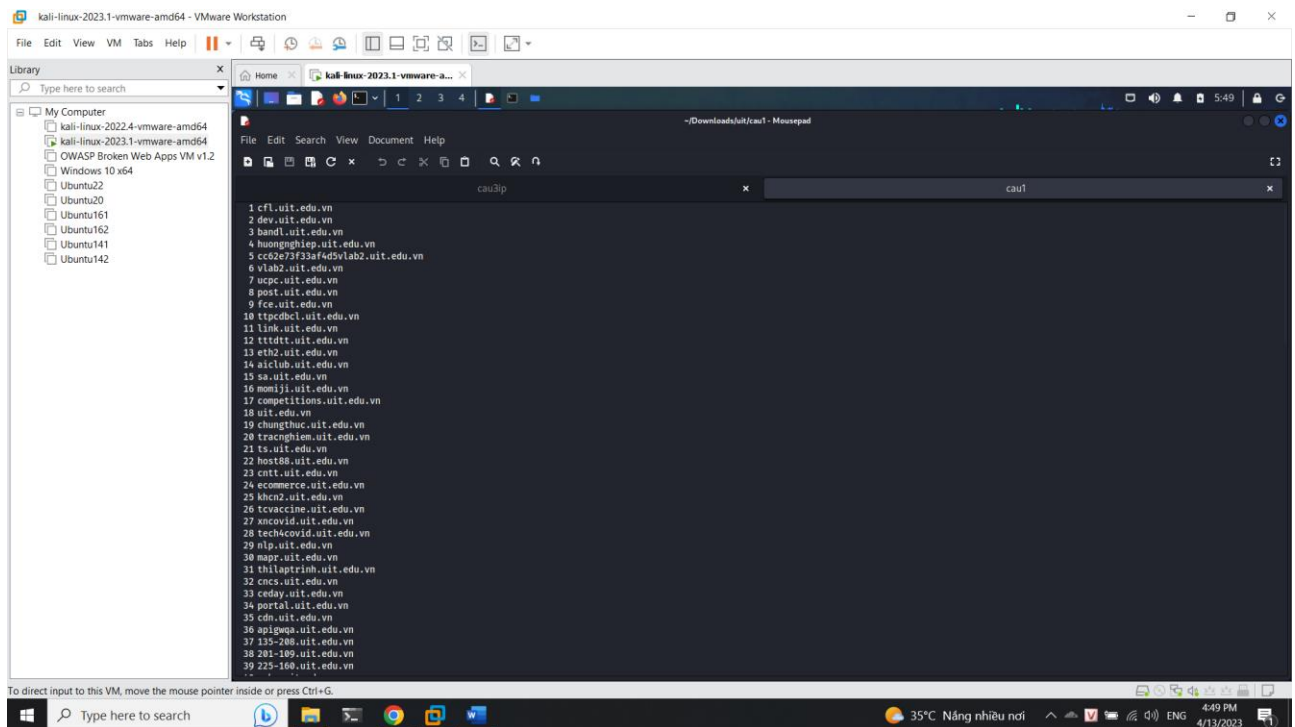
1. Kịch bản 01

Đầu tiên ta vào trang virustotal để thực hiện kiểm tra các subdomain có được từ domain uit.edu.vn thì ta thấy được 127 kết quả

<https://www.virustotal.com/gui/domain/uit.edu.vn/rerelations>



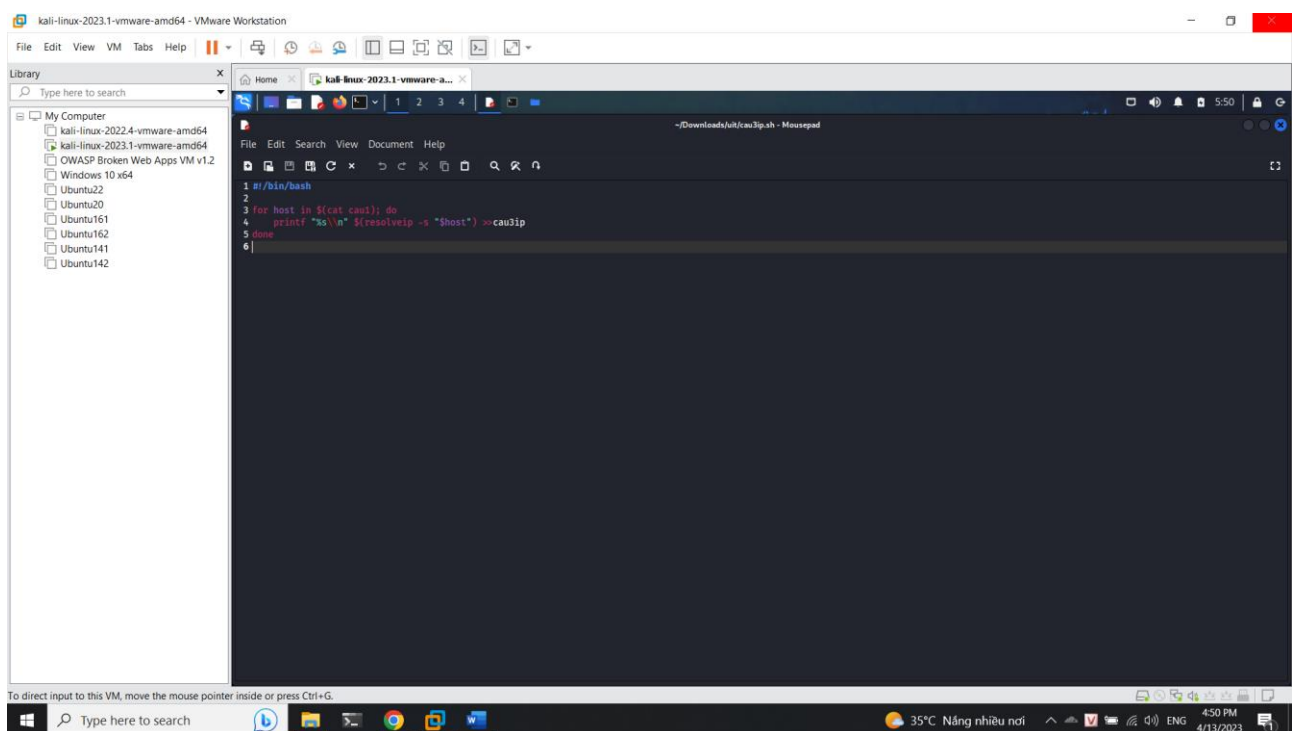
Sau đó ta sẽ copy kết quả bỏ vào file text để thực hiện cho bước tiếp theo



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. A text editor window is open, displaying a list of subdomains for 'uit.edu.vn'. The list includes: cfl.uit.edu.vn, dev.uit.edu.vn, band1.uit.edu.vn, huongnghiep.uit.edu.vn, cc62e73f3af4d5d5lab2.uit.edu.vn, vlab2.uit.edu.vn, wpc.uit.edu.vn, post.uit.edu.vn, fce.uit.edu.vn, ttpodcl.uit.edu.vn, link.uit.edu.vn, ttdtt.uit.edu.vn, eth2.uit.edu.vn, siclub.uit.edu.vn, sa.uit.edu.vn, momiji.uit.edu.vn, competitions.uit.edu.vn, uit.edu.vn, chungthuc.uit.edu.vn, tracnghiem.uit.edu.vn, ts.uit.edu.vn, host88.uit.edu.vn, cntt.uit.edu.vn, ecommerce.uit.edu.vn, khcn2.uit.edu.vn, tvaccclm.uit.edu.vn, encovid.uit.edu.vn, tech4covid.uit.edu.vn, nlp.uit.edu.vn, npr.uit.edu.vn, thilaptrinh.uit.edu.vn, cncs.uit.edu.vn, ceday.uit.edu.vn, portal.uit.edu.vn, edn.uit.edu.vn, apigwqa.uit.edu.vn, 135-208.uit.edu.vn, 201-109.uit.edu.vn, 225-160.uit.edu.vn, and so on.

2. Kịch bản 02

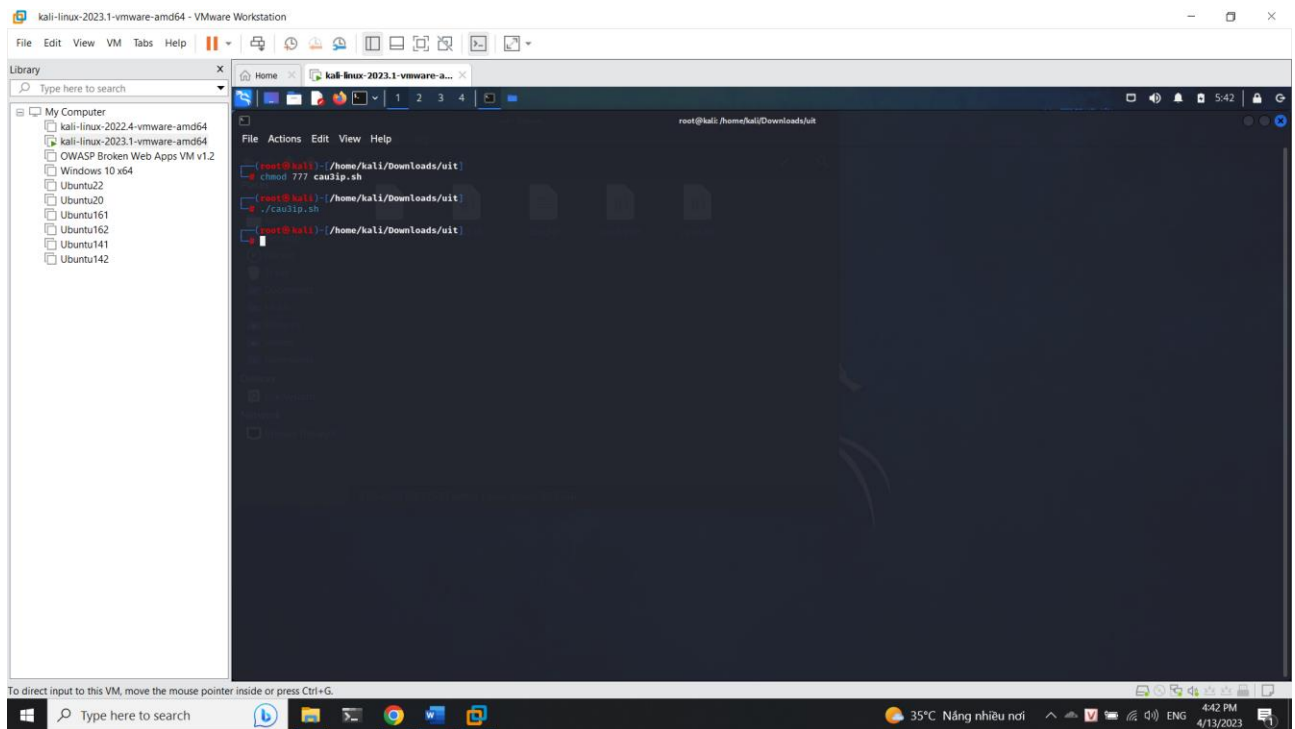
Tiếp theo ta sẽ thực hiện dò tìm ip của các subdomain mà ta tìm được, đầu tiên ta cần phải thực hiện tạo shell code, ở đây chương trình sẽ lấy mỗi subdomain sau đó thực hiện resolve ip để trả về kết quả ip



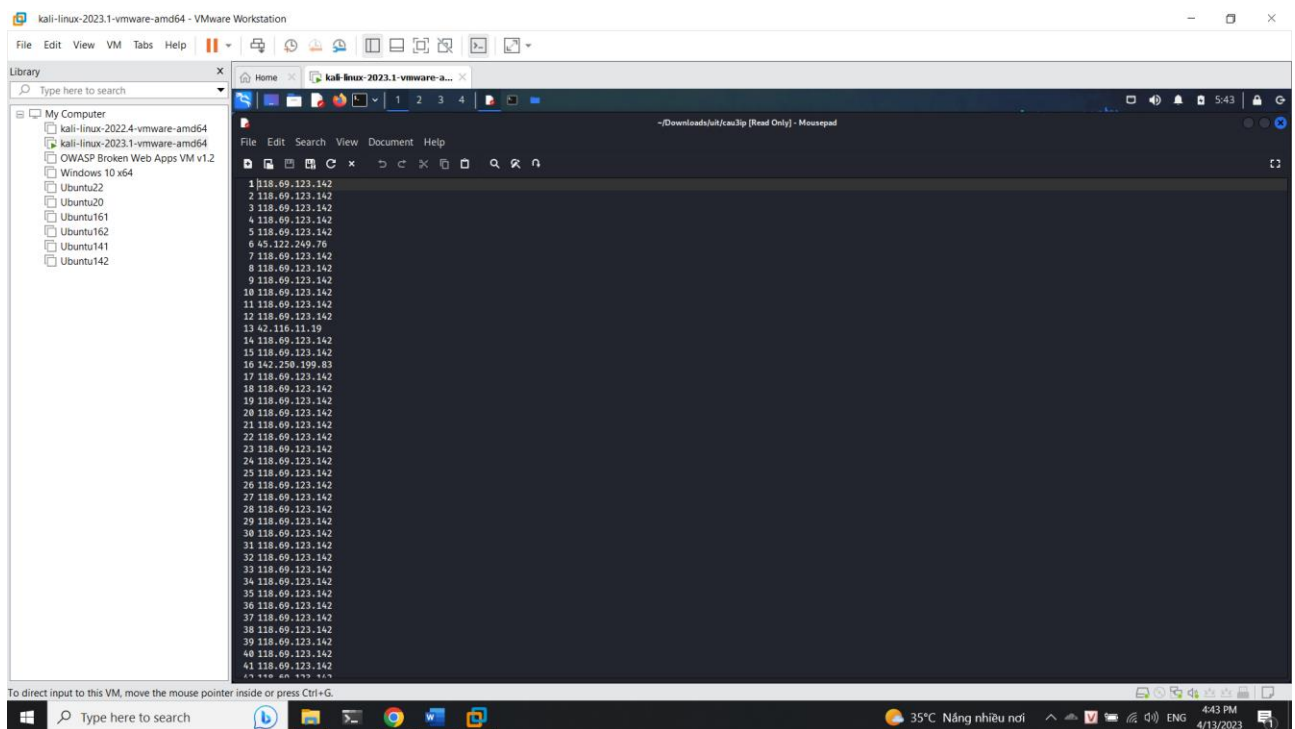
The screenshot shows the same Kali Linux VM. A shell script named 'cau3ip.sh' is open in a text editor. The script contains the following code:

```
1 #!/bin/bash
2
3 for host in $(cat cau1); do
4     printf "%s\n" $(resolveip -s "$host") >>cau3ip
5 done
6
```

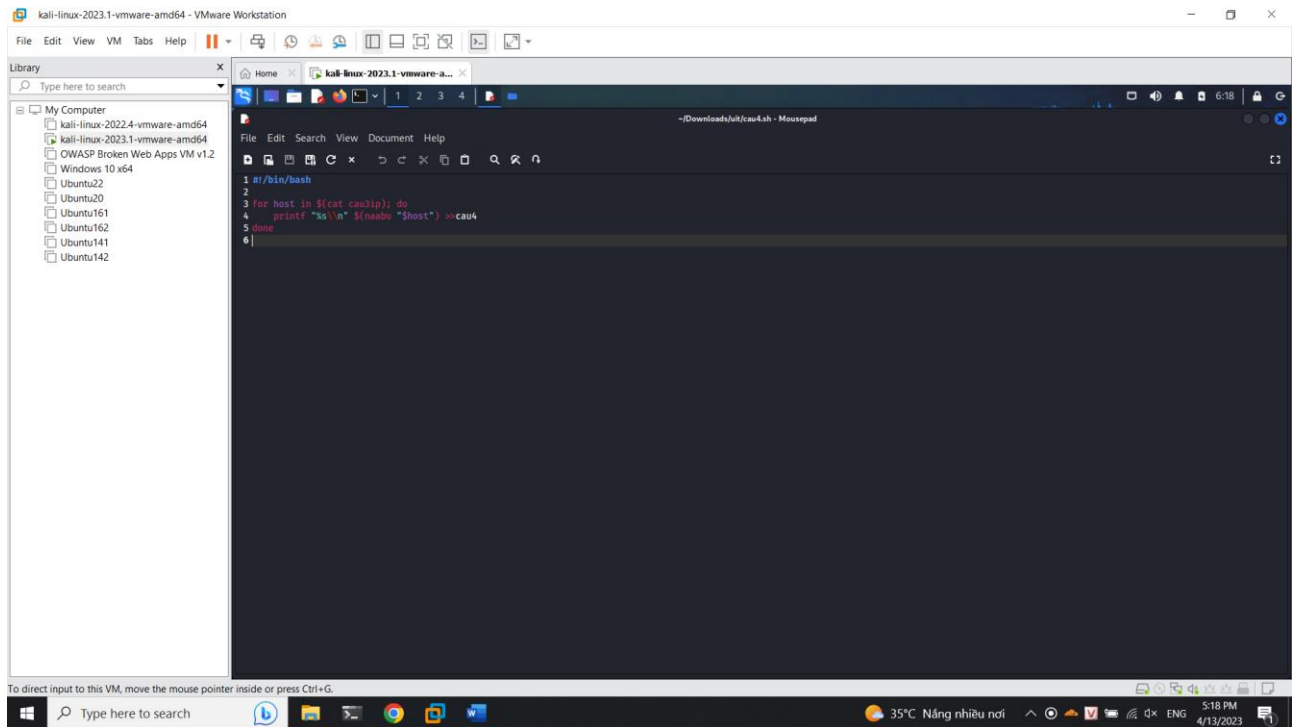
Cấp toàn quyền cho file shell code, thực hiện chạy với quyền root trên máy tính lệnh vừa tạo



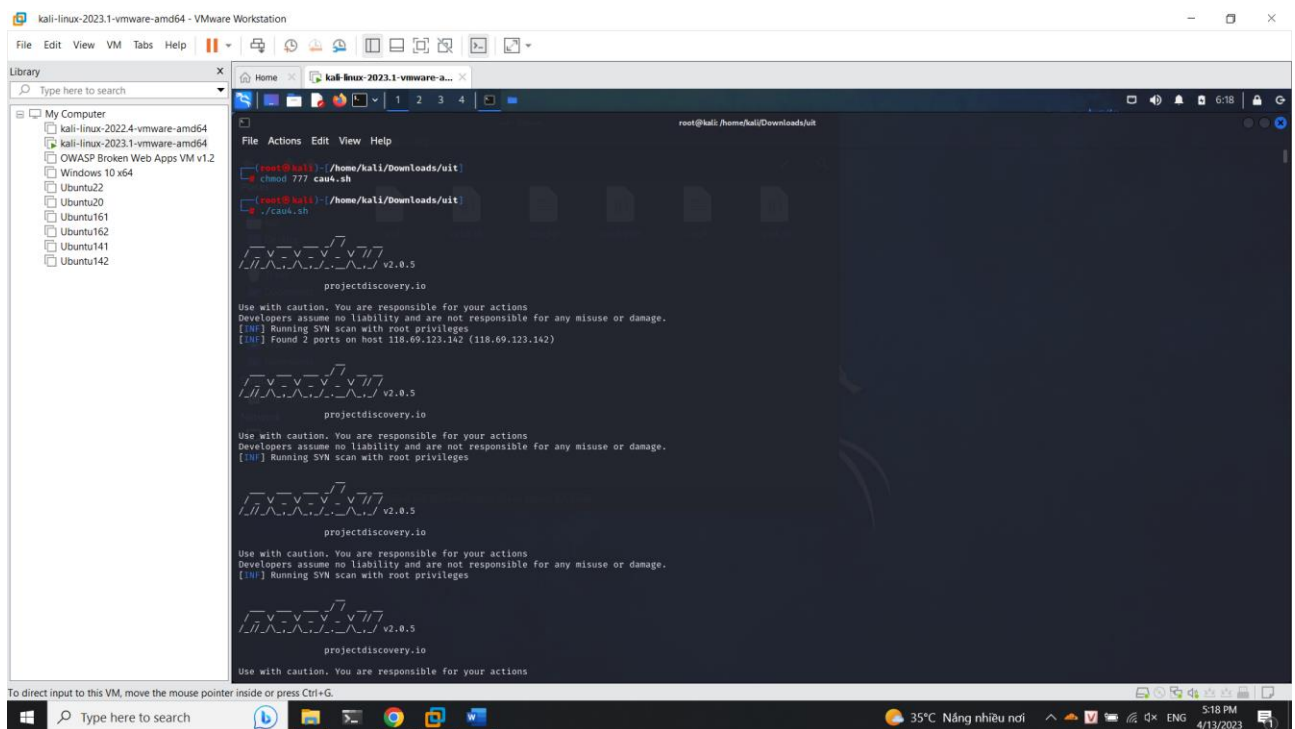
Sau khi chạy xong ta có kết quả là dãy ip bên dưới



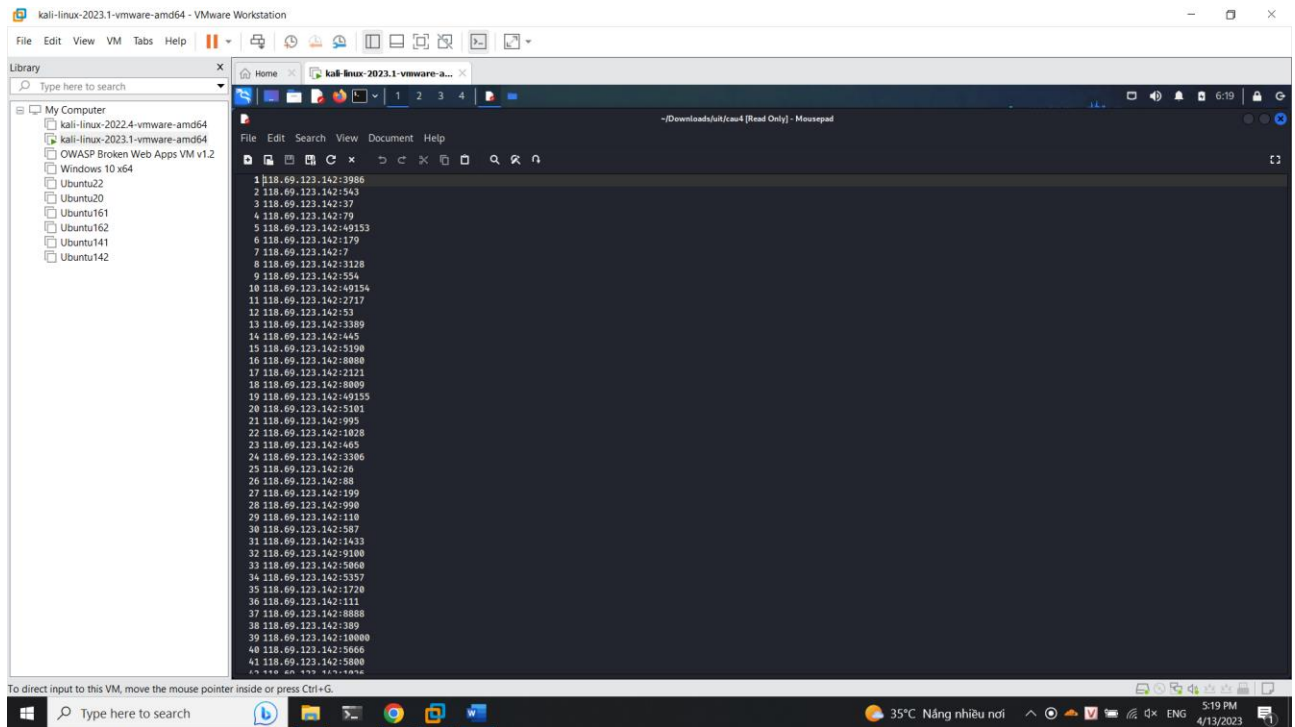
Tiếp tục ta sẽ thực hiện việc tạo code để tìm port đang mở của các ip đã tìm được, ở đây đoạn code sẽ lấy mỗi ip ra để scan các port đang mở



Cấp toàn quyền cho file code và thực hiện với quyền root

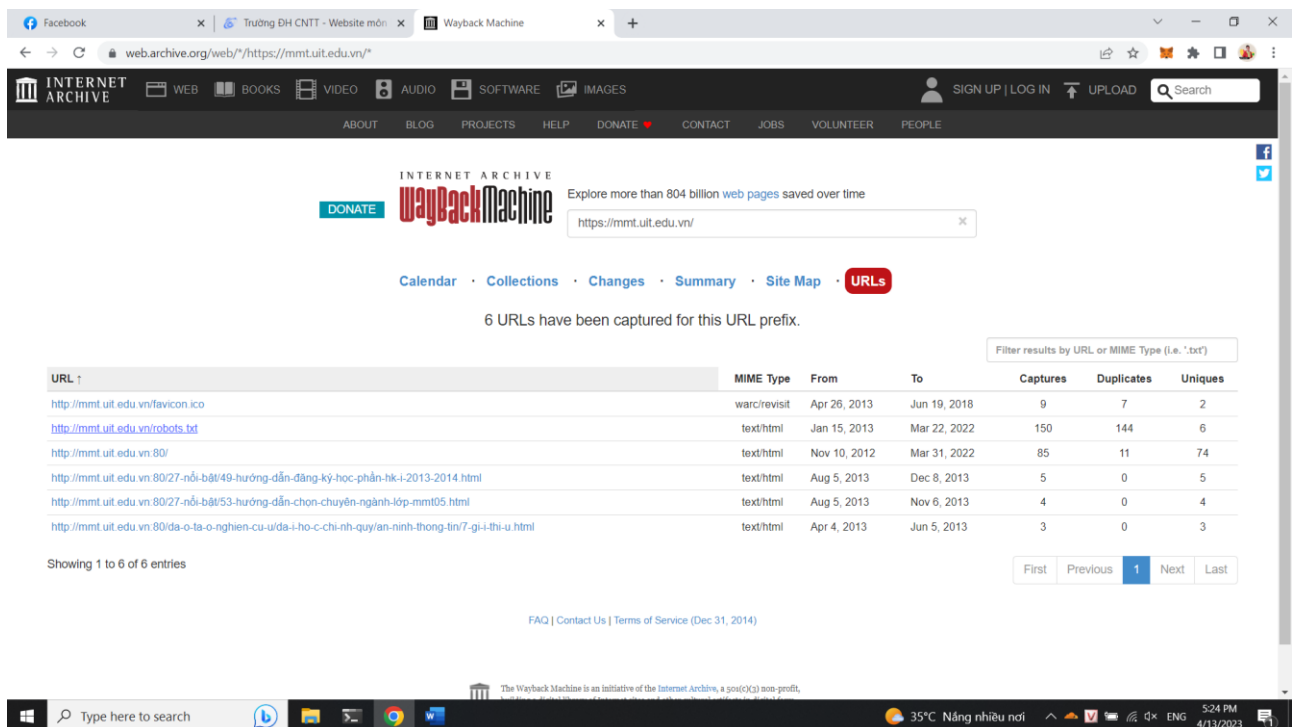


Sau khi chạy xong ta sẽ có được kết quả như hình

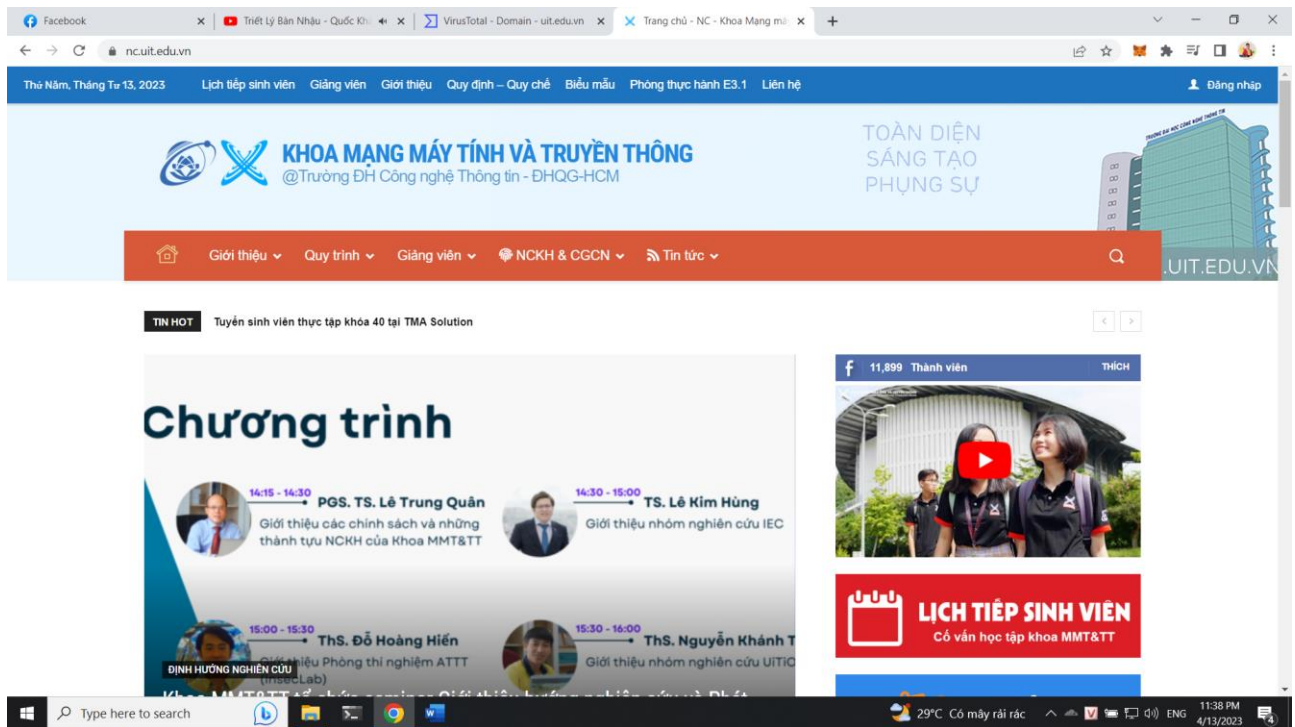


3. Kịch bản 03

Ở đây ta tìm kiếm các thông tin về các domain đã ngưng hoạt động ta thấy được domain mmt.uit.edu.vn đã dừng hoạt động



Và khi truy cập vào trang sẽ được trở sang trang nc.uit.edu.vn

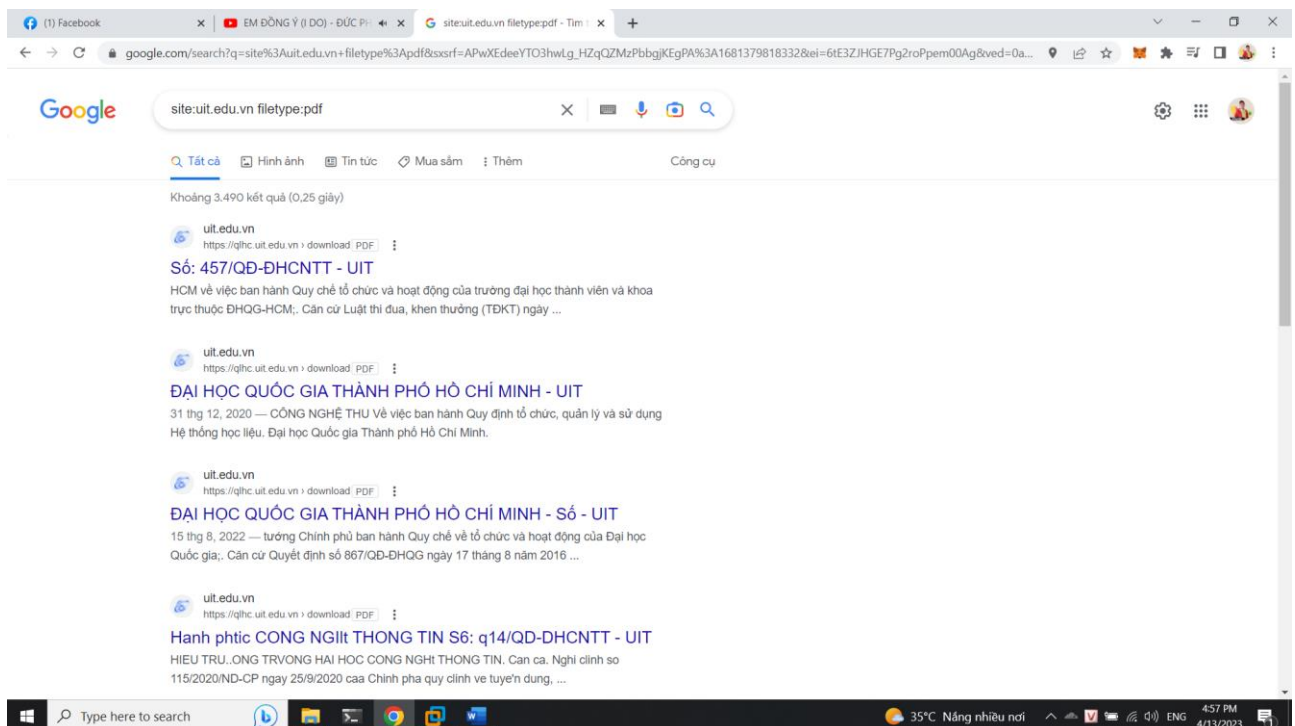


4. Kịch bản 04

Google dork

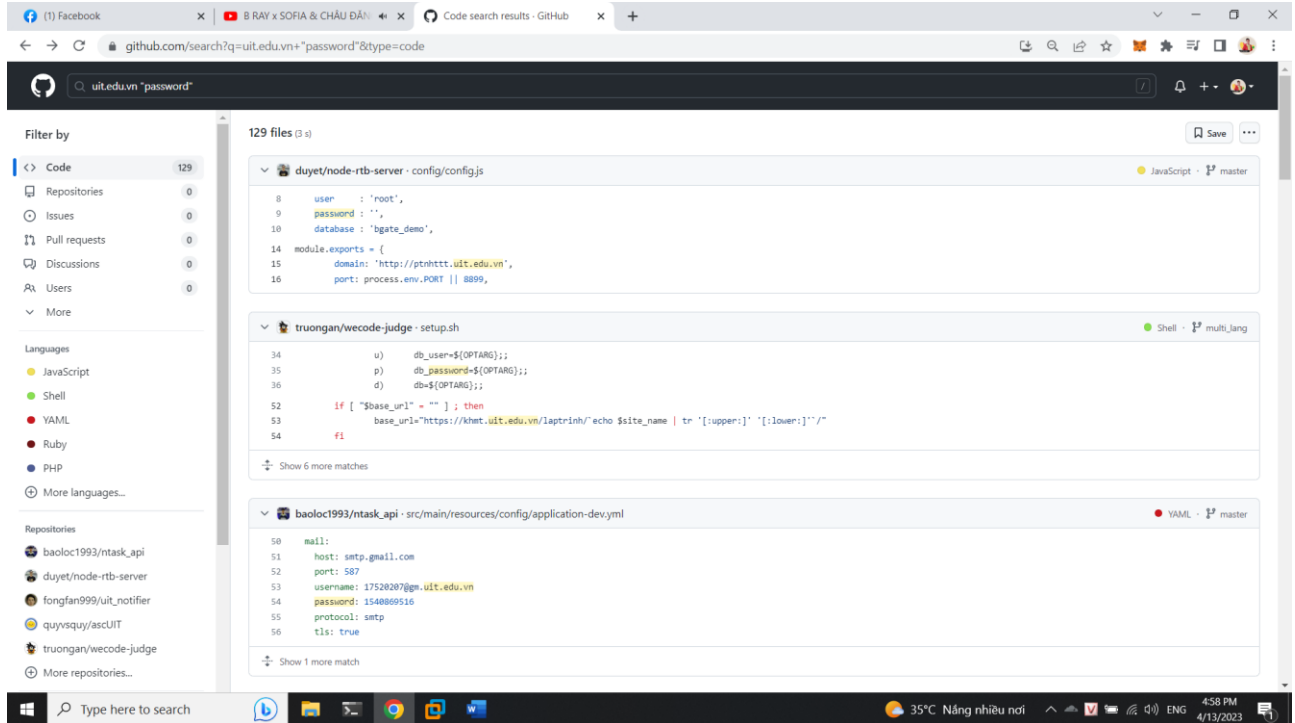
Đầu tiên ở phần dữ liệu nhạy cảm với google dork ta sẽ thực hiện theo phương pháp manual bằng cách nhập và thanh tìm kiếm:

Site:uit.edu.vn filetype:pdf ta có thể thấy được một số trang có chứa file pdf



Github dork

Tiếp tục thực hiện tìm kiếm trên github dork bằng phương pháp manual thì ta sẽ thực hiện lệnh: `uit.edu.vn "password"` thì ta thấy được một số thông tin password được liệt kê trên các phần code của một số cá nhân thuộc UIT



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