

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 xóa 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

2. NỘI DUNG THỰC HIỆN: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.

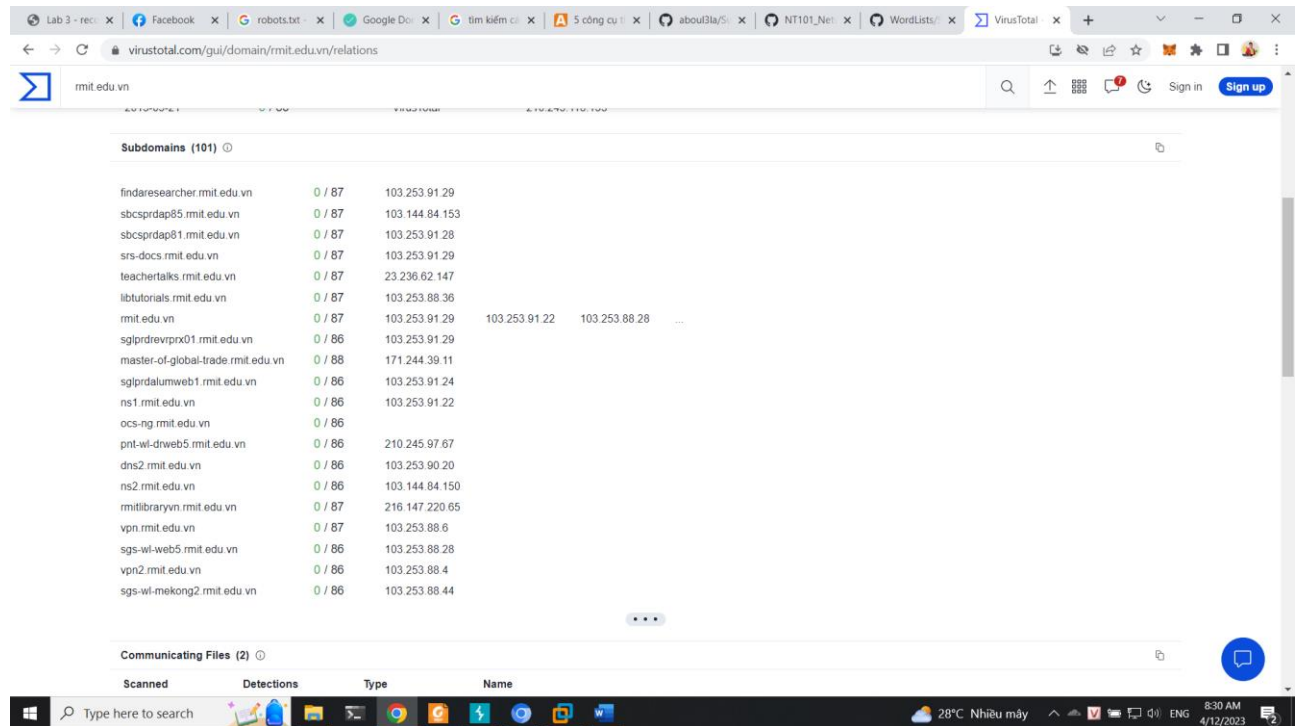
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. 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>



2. Kịch bản 2

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

The screenshot shows the Burp Suite interface. The top tab is 'Attack', and the 'Results' tab is active, displaying a list of requests. The first request is a GET request to 'http://www.rmit.edu.vn' with a status of 200. Below the list, the 'Request' tab is selected, showing the raw HTTP request. The request includes a Host header, a Cookie, and various user-agent and accept headers. The status bar at the bottom indicates 'Finished'.

Request	Payload	Target	Status	Error	Timeout	Length	Comment
1	www	https://www.rmit.edu.vn	200			374364	
450	careers	https://careers.rmit.edu.vn	404			32452	
477	lms	https://lms.rmit.edu.vn	505			354	
0		https://subdomain.rmit.edu.vn					baseline request
2	mail	https://mail.rmit.edu.vn					
3	ftp	https://ftp.rmit.edu.vn					
4	localhost	https://localhost.rmit.edu.vn					
5	webmail	https://webmail.rmit.edu.vn					
6	smtp	https://smtp.rmit.edu.vn					
7	webdisk	https://webdisk.rmit.edu.vn					
8	pop	https://pop.rmit.edu.vn					
9	cpanel	https://cpanel.rmit.edu.vn					
10	whm	https://whm.rmit.edu.vn					
11	ns1	https://ns1.rmit.edu.vn					
12	ns2	https://ns2.rmit.edu.vn					

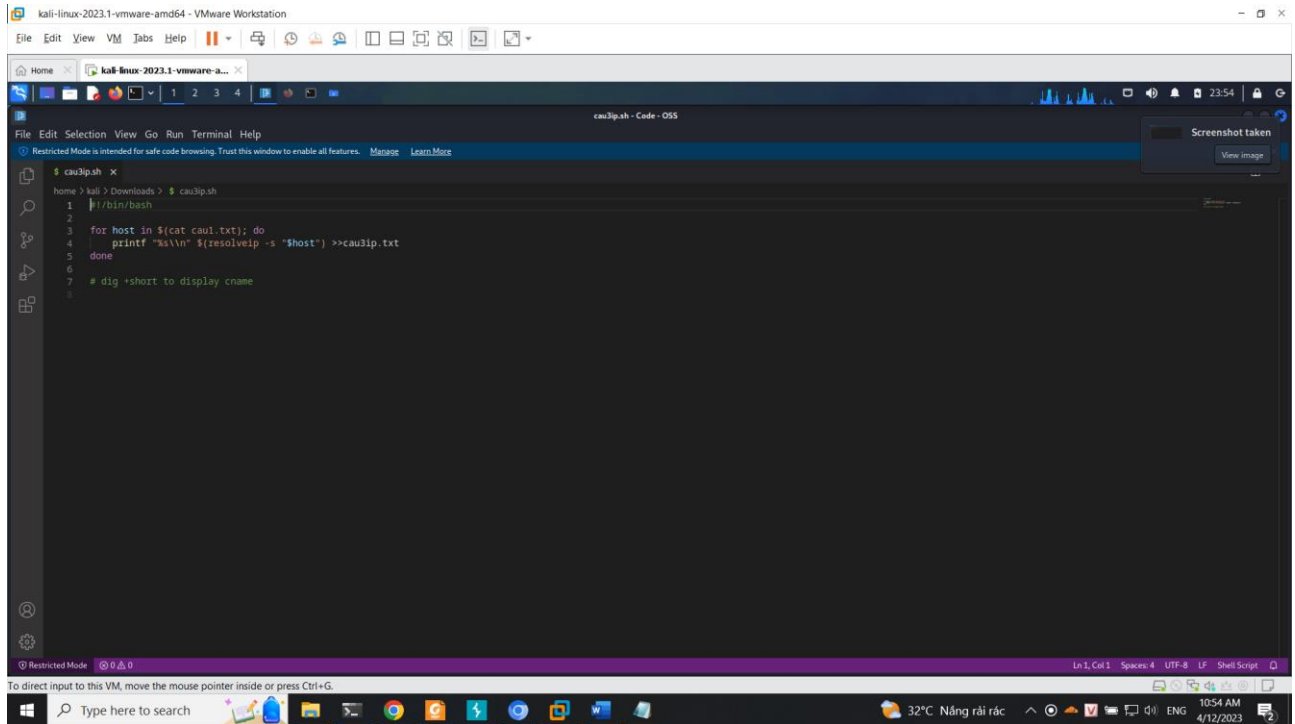
Ngoài ra ta có thể thực hiện việc tấn công bằng các payload được filter lại từ các subdomain tìm được ở câu 1 và thực hiện tấn công, ở đây ta thấy được rằng là để lọc được các thông tin như là status thì ta sẽ ấn vào trường status, điều này sẽ khiến cho việc lọc status dễ dàng hơn

The screenshot shows the Burp Suite interface. The top tab is 'Attack', and the 'Results' tab is active, displaying a list of requests. The first request is a GET request to 'http://findaresearcher.rmit.edu.vn' with a status of 200. Below the list, the 'Request' tab is selected, showing the raw HTTP request. The request includes a Host header, a Cookie, and various user-agent and accept headers. The status bar at the bottom indicates 'Finished'.

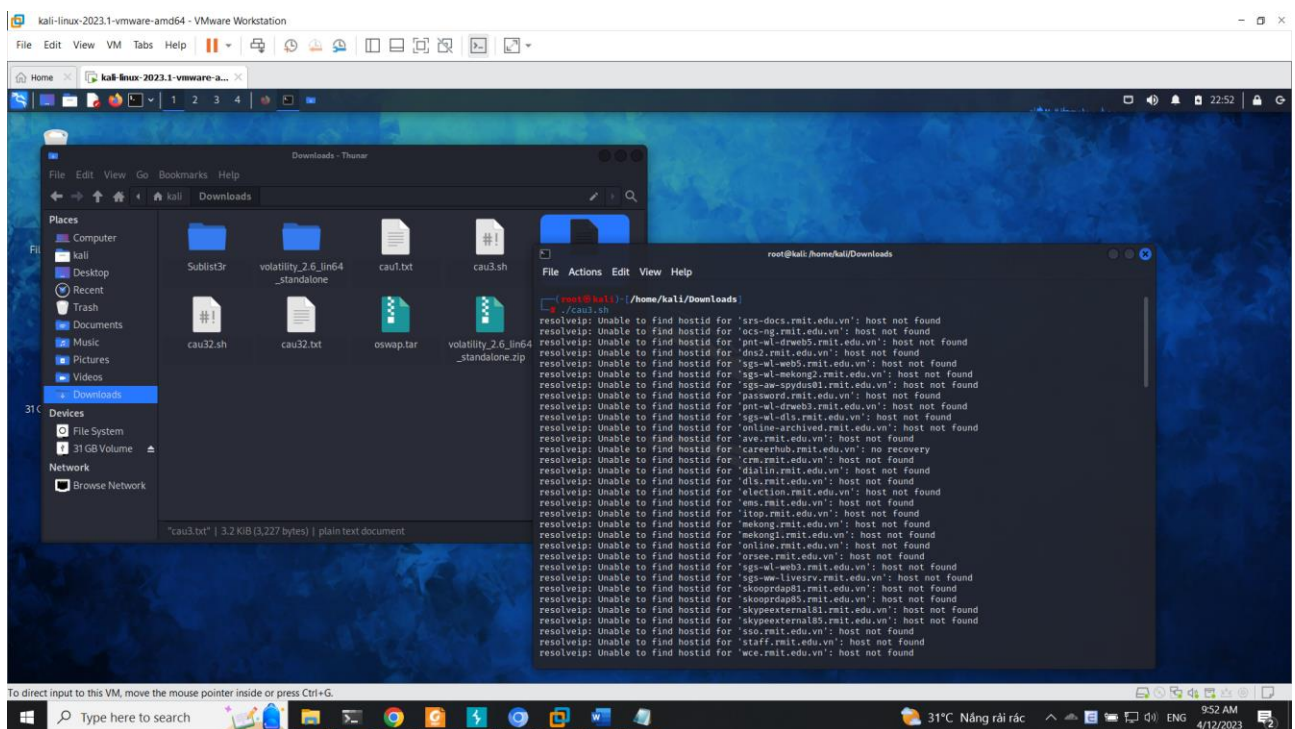
Request	Payload	Target	Status	Error	Timeout	Length	Comment
1	findaresearcher	https://findaresearcher.rmit.edu.vn	200			1101	
6	libtutorials	https://libtutorials.rmit.edu.vn	200			2064	
10	sglprdalumweb1	https://sglprdalumweb1.rmit.edu.vn	200			292	
75	sas	https://sas.rmit.edu.vn	200			2137	
78	pe	https://pe.rmit.edu.vn	200			4146	
80	omeka	https://omeka.rmit.edu.vn	200			28837	
94	design	https://design.rmit.edu.vn	200			1764	
96	chame	https://chame.rmit.edu.vn	200			132474	
99	etal	https://etal.rmit.edu.vn	200			2117	
101	www	https://www.rmit.edu.vn	200			374366	
5	teachertalks	https://teachertalks.rmit.edu.vn	301			821	
83	event	https://event.rmit.edu.vn	301			814	
95	infosession	https://infosession.rmit.edu.vn	301			773	
98	library	https://library.rmit.edu.vn	301			372	
100	rmitenglishevent	https://rmitenglishevent.rmit.edu.vn	301			825	
8	sglprdevrpn01	https://sglprdevrpn01.rmit.edu.vn	302			876	
16	rmitlibraryvn	https://rmitlibraryvn.rmit.edu.vn	302			556	
81	typographyvn	https://typographyvn.rmit.edu.vn	302			540	
97	rvf2020	https://rvf2020.rmit.edu.vn	302			207	
24	sgs-wl-omeka	https://sgs-wl-omeka.rmit.edu.vn	403			430	
92	emedia	https://emedia.rmit.edu.vn	403			4319	
63	sip	https://sip.rmit.edu.vn	404			294	
0		https://domain.rmit.edu.vn					baseline request

3. Kịch bản 3

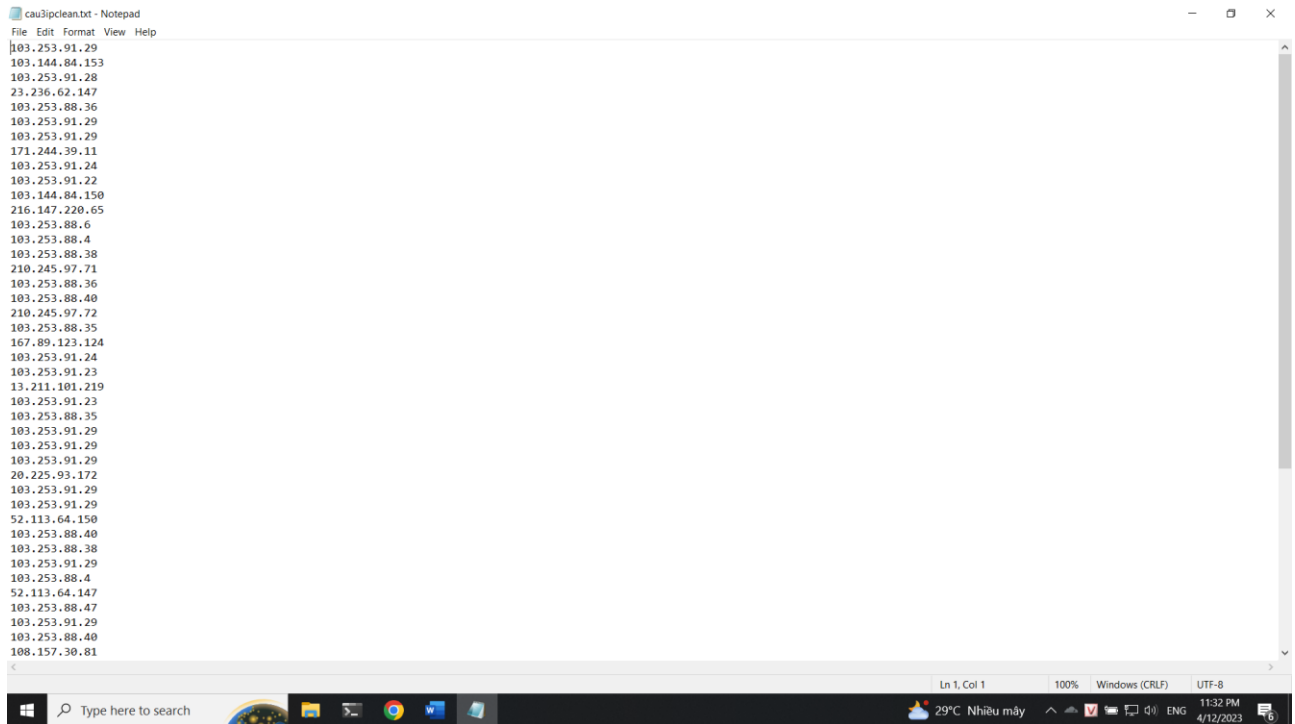
Đầu tiên ta sẽ thực hiện tạo shell như hình để có thể lấy được ip, ý nghĩa: với mỗi host trong file cau1.txt thì ta sẽ resolve ip ra từ host đó và gán vào file cau3ip



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



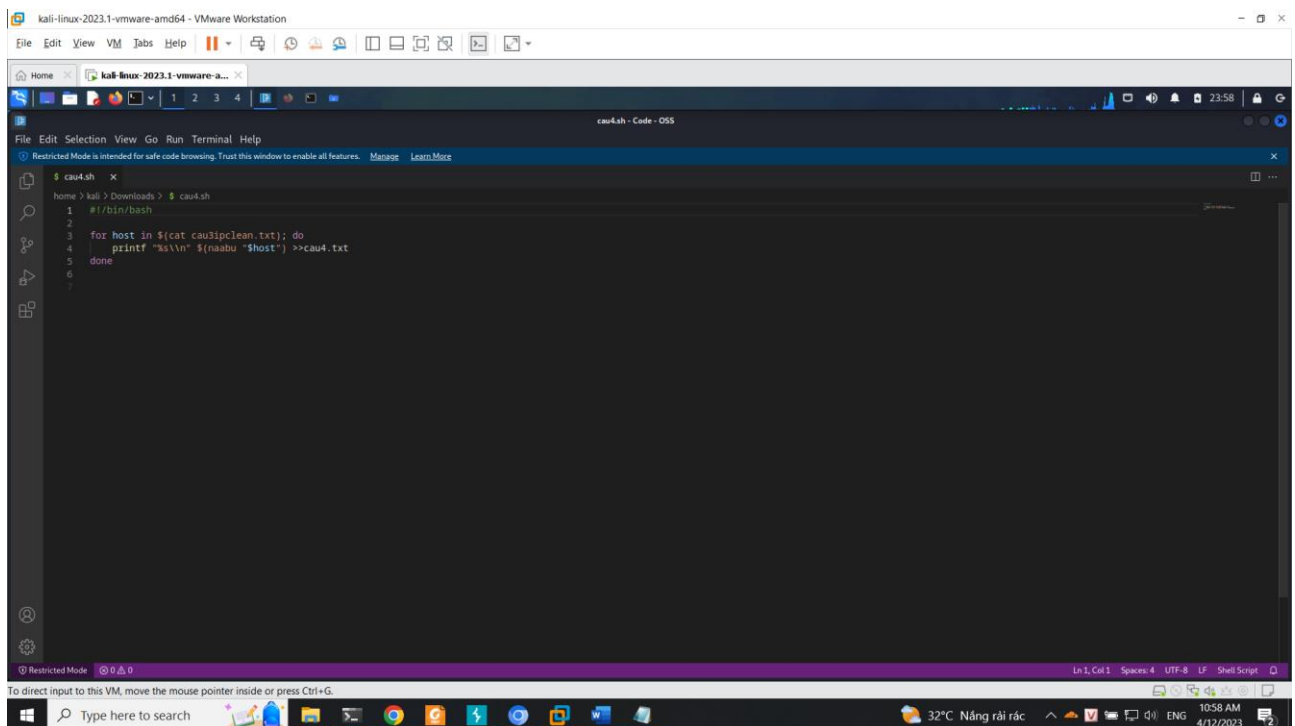
Sau khi thực hiện xong và filter lại file thì ta có kết quả



```
caulpclean.txt - Notepad
File Edit Format View Help
103.253.91.29
103.144.84.153
103.253.91.28
23.236.62.147
103.253.88.36
103.253.91.29
103.253.91.29
171.244.39.11
103.253.91.24
103.253.91.22
103.144.84.150
216.147.220.65
103.253.88.6
103.253.88.4
103.253.88.38
210.245.97.71
103.253.88.36
103.253.88.40
210.245.97.72
103.253.88.35
167.89.123.124
103.253.91.24
103.253.91.23
13.211.101.219
103.253.91.23
103.253.88.35
103.253.91.29
103.253.91.29
103.253.91.29
20.225.93.172
103.253.91.29
103.253.91.29
52.113.64.150
103.253.88.40
103.253.88.38
103.253.91.29
103.253.88.4
52.113.64.147
103.253.88.47
103.253.91.29
103.253.88.40
108.157.30.81
```

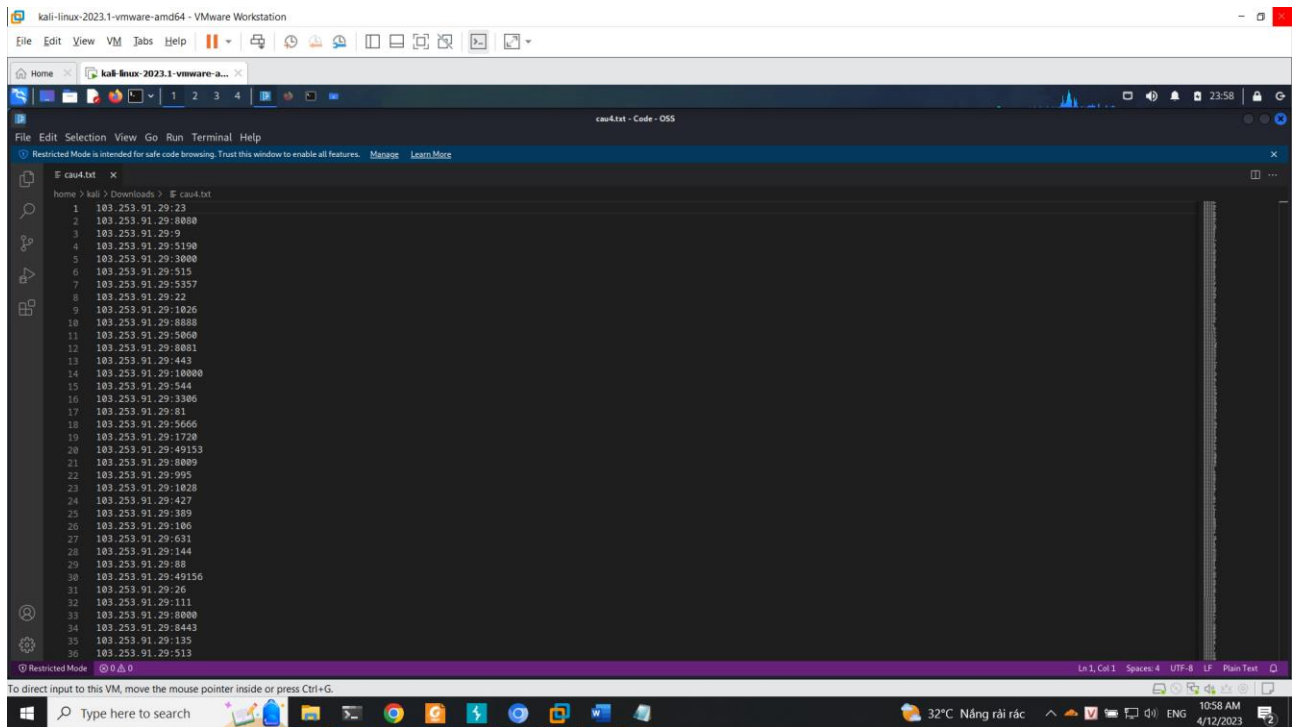
4. Kịch bản 4

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



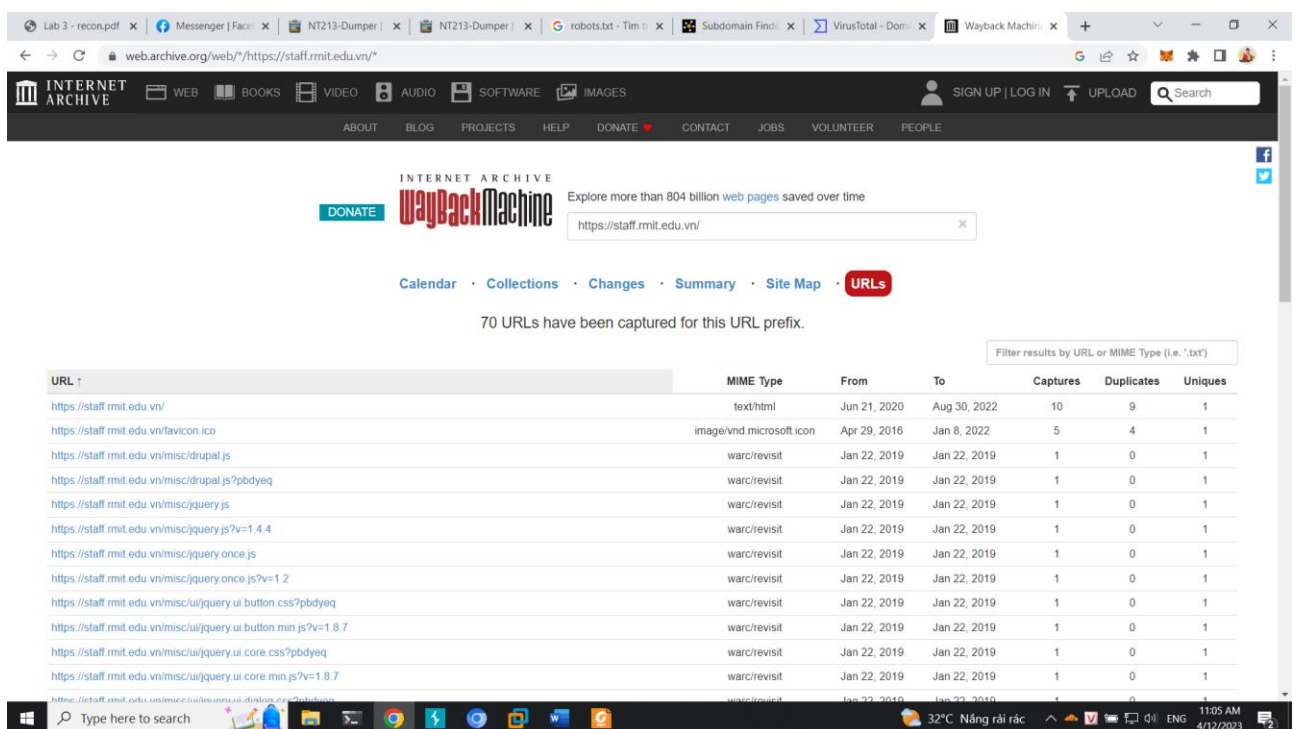
```
kali-linux-2023.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
cau4.sh - Code - OSS
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
$ cau4.sh
home > kali > Downloads > $ cau4.sh
1 #!/bin/bash
2
3 for host in $(cat caulpclean.txt); do
4     printf "%s\\n" $(naabu -h$host) >>cau4.txt
5 done
6
```

Sau khi thực hiện xong thì ta có được kết quả



5. 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

The screenshot shows the Wayback Machine search results for the URL `https://emedia.rmit.edu.vn/`. The interface includes a search bar, navigation links (Calendar, Collections, Changes, Summary, Site Map, URLs), and a table of captured URLs.

URL	MIME Type	From	To	Captures	Duplicates	Uniques
http://emedia.rmit.edu.vn/80/media/author/writersWorkshop/businessComputing/Business Computing Writers' Workshop/story.html	text/html	Apr 25, 2017	Aug 1, 2017	4	3	1
https://emedia.rmit.edu.vn/media/author/commercialLawWriting/story.html	text/html	Jan 26, 2022	Dec 7, 2022	2	1	1
https://emedia.rmit.edu.vn/media/author/Technical Report Writing/story.html	text/html	Aug 1, 2021	Aug 1, 2021	1	0	1

Showing 1 to 3 of 3 entries

6. 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

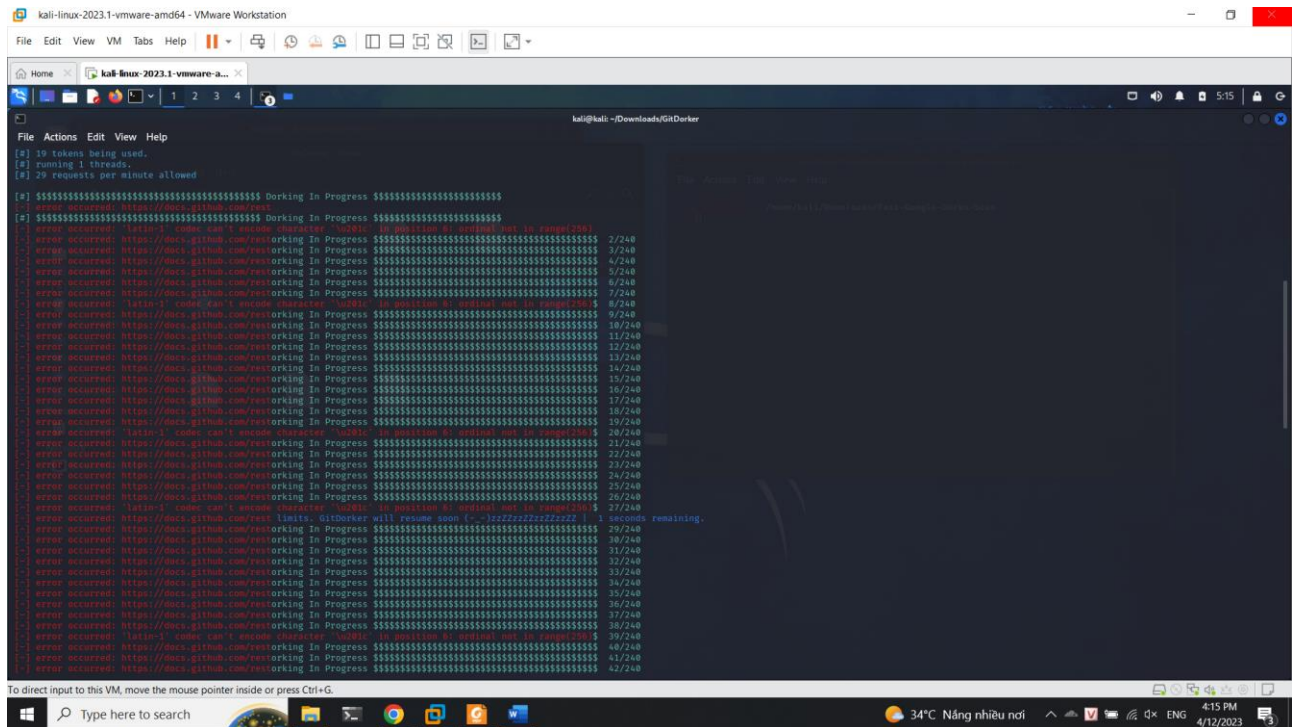
site:alumninetwork.rmit.edu.vn filetype:pdf OR filetype:doc OR filetype:xls

The screenshot shows Google search results for the query `site:alumninetwork.rmit.edu.vn filetype:pdf OR filetype:doc OR filetype:xls`. The results list several documents from RMIT Alumninetwork, including:

- Welcome to our Partnership Program - RMIT Alumni Network** (PDF)
- RMIT Vietnam Alumni Connecting the dots** (PDF)
- RMIT Alumni 2021 - Beyond the Borders** (PDF)
- RMIT ALUMNI RECAP 2022** (PDF)

7. 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

Võ Anh Kiệt

9:37 PM

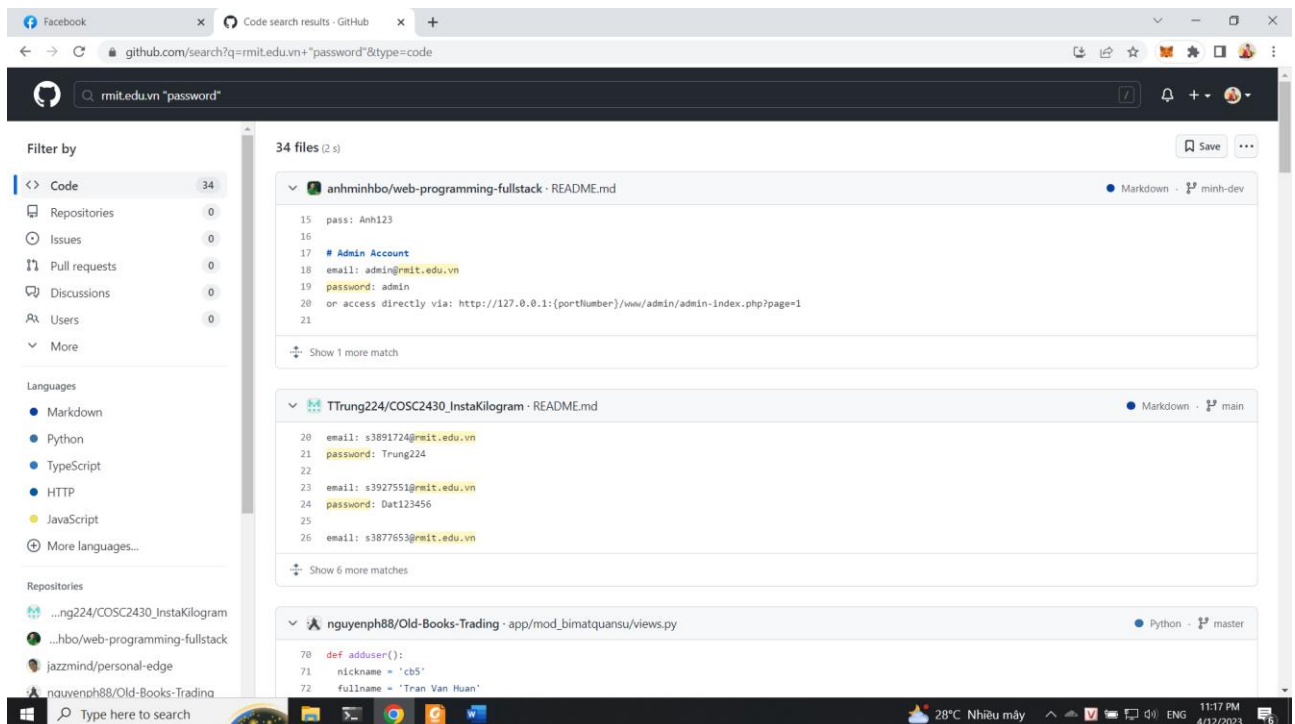
Chào các thầy và các bạn, hiện tại thì em/minh đang làm câu 7 sử dụng tool GitDorker, chạy lệnh như hình 1 thì sau khi chạy hoàn thành thì chương trình báo bug liên quan đến name not defined như hình 2, phiên bản python hiện tại đang sử dụng là 3.10. Em/minh mong nhận được sự hỗ trợ của các thầy, các bạn và bạn **Tô Đình Nguyễn**

[See less](#)

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


```
Traceback (most recent call last):$$$$$$$$$ Dorking In Progress $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$ 3/240
File "GitDorker.py", line 325, in <module>
    pool.map(api_search, url_dict)
File "/usr/lib/python3.6/multiprocessing/pool.py", line 266, in map
    return self._map_async(func, iterable, mapstar, chunksize).get()
File "/usr/lib/python3.6/multiprocessing/pool.py", line 644, in get
    raise self._value
File "/usr/lib/python3.6/multiprocessing/pool.py", line 119, in worker
    result = (True, func(*args, **kwargs))
File "/usr/lib/python3.6/multiprocessing/pool.py", line 44, in mapstar
    return list(map(*args))
File "GitDorker.py", line 164, in api_search
    headers = {"Authorization": "token " + token_round_robin()}
File "GitDorker.py", line 140, in token_round_robin
    current_token = tokens_list[n]
IndexError: list index out of range
```

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



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