

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng

Tên chủ đề: Lab 3 - Reconnaissance

GVHD: Ngô Đức Hoàng Sơn

Nhóm: 14

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.O21.ANTT.1

STT	Họ và tên	MSSV	Email
1	Vũ Tuấn Sơn	21521389	21521389@gm.uit.edu.vn
2	Bùi Đức Anh Tú	21522735	21522735@gm.uit.edu.vn
3	Lê Huy Hiệp	21522067	21522067@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	90%	1 - 3
2	Yêu cầu 2	50%	3 - 5
3
Điểm tự đánh giá			?/10

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

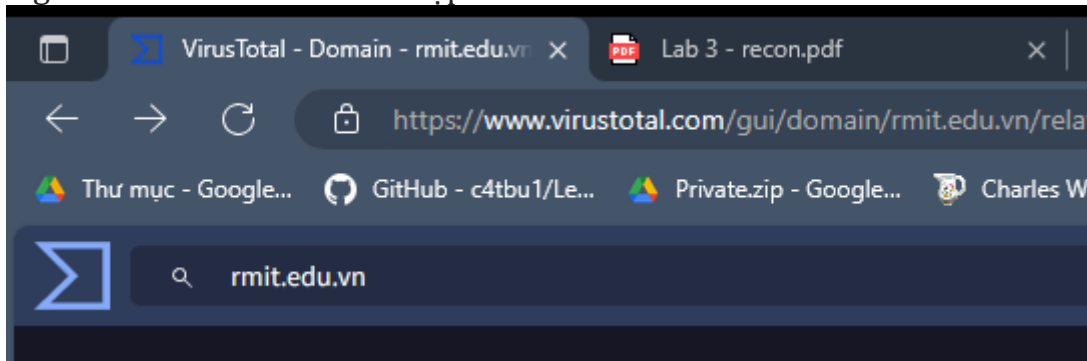
BÁO CÁO CHI TIẾT

1. Subdomain Enumeration

a) Liệt kê thông qua các nguồn trên Internet:

Bài tập 1: Liệt kê ra ít nhất 100 tên miền phụ của rmit.edu.vn, kết quả được lưu trong file csv.

Vào trang web virustotal.com và nhập tên miền “rmit.edu.vn”:



Từ kết quả của VirusTotal, ta tìm được 102 subdomain của tên miền rmit.edu.vn:

2013-05-21	0 / 90	VirusTotal	210.245.118.133
Subdomains (102)			
password-assistance.rmit.edu.vn	0 / 90	103.253.91.29	
findaresearcher.rmit.edu.vn	0 / 90	103.253.91.29	
sbcsp85.rmit.edu.vn	0 / 90	103.144.84.153	
sbcsp81.rmit.edu.vn	0 / 90	103.253.91.28	
srs-docs.rmit.edu.vn	0 / 90	103.253.91.29	
teachertalks.rmit.edu.vn	0 / 90	23.236.62.147	
libtutorials.rmit.edu.vn	0 / 90	103.253.88.36	
sglprdevrpx01.rmit.edu.vn	0 / 90	103.253.91.29	
master-of-global-trade.rmit.edu.vn	0 / 90	171.244.39.11	
sglpralumweb1.rmit.edu.vn	0 / 90	103.253.91.24	
ns1.rmit.edu.vn	0 / 90	103.253.91.22	
ocs-ng.rmit.edu.vn	0 / 90		
pnt-wl-drweb5.rmit.edu.vn	0 / 90	210.245.97.67	
dns2.rmit.edu.vn	0 / 90	103.253.90.20	
ns2.rmit.edu.vn	0 / 90	103.144.84.150	

Ta copy các tên miền vừa tìm được vào 1 file .csv để chuẩn bị cho các bước tiếp theo:

```

File Actions Edit View Help

(kali@kali)-[~]
$ cat 100rmitDomain.csv
password-assistance.rmit.edu.vn
findaresearcher.rmit.edu.vn
sbcsprdap85.rmit.edu.vn
sbcsprdap81.rmit.edu.vn
srs-docs.rmit.edu.vn
teachertalks.rmit.edu.vn
libtutorials.rmit.edu.vn
sglprdrevrprx01.rmit.edu.vn
master-of-global-trade.rmit.edu.vn
sglprdalumweb1.rmit.edu.vn
ns1.rmit.edu.vn
ocs-ng.rmit.edu.vn
pnt-wl-drweb5.rmit.edu.vn
dns2.rmit.edu.vn
ns2.rmit.edu.vn
rmitlibraryvn.rmit.edu.vn
vpn.rmit.edu.vn
sgs-wl-web5.rmit.edu.vn
vpn2.rmit.edu.vn
sgs-wl-mekong2.rmit.edu.vn
sgs-aw-spydus01.rmit.edu.vn
sgs-aw-hrapp1.rmit.edu.vn
drwprdhrapp01.rmit.edu.vn
sgs-wl-omeka.rmit.edu.vn

```

b) Tìm kiếm chủ động tên miền thông qua kỹ thuật brute-force

Bài tập 2: Dựa vào các tên miền phụ đã tìm kiếm được ở bài tập 1 và các tên miền đã bruteforce được thêm bằng burpsuite intruder. Phân loại các tên miền có kết quả trả về status code 200 và các tên miền có kết quả trả về khác.

Thực hiện request tới rmit.edu.vn thông qua trình duyệt của Burpsuite:

Host	Method
https://www.rmit.edu.vn	GET
https://www.rmit.edu.vn	GET
https://www.rmit.edu.vn	GET
https://www.rmit.edu.vn	GET
https://www.rmit.edu.vn	GET
https://www.rmit.edu.vn	GET
https://www.rmit.edu.vn	GET
https://www.rmit.edu.vn	GET

Chuột phải chọn 1 request và chọn Send to Intruder:

Host	Method	URL	Params	Status C
https://www.rmit.edu.vn	GET			200
https://www.rmit.edu.vn	GET	https://www.rmit.edu.vn/		
https://www.rmit.edu.vn	GET	Add to scope		
https://www.rmit.edu.vn	GET	Scan		
https://www.rmit.edu.vn	GET	Send to Intruder	Ctrl+I	✓
https://www.rmit.edu.vn	GET	Send to Repeater	Ctrl+R	
https://www.rmit.edu.vn	GET	Send to Sequencer		
https://www.rmit.edu.vn	GET	Send to Organizer	Ctrl+O	

Làm theo hướng dẫn các bước trong link tại [đây](#) với payload là file .csv được tạo ra từ các subdomain đã tìm thấy bên trên để tiến hành tìm các tên miền có thể truy cập được (status code 200):

The screenshot shows the Burp Suite Intruder interface. The 'Intruder' tab is selected, and the 'Payloads' sub-tab is active. The 'Payload set' is set to '1' and the 'Payload type' is 'Simple list'. The 'Request count' is 102. The 'Payload settings [Simple list]' section shows a list of subdomains: pnt-wl-drweb3.rmit.edu.vn, english.rmit.edu.vn, email.rmit.edu.vn, alumninetwork.rmit.edu.vn, sgs-wl-dls.rmit.edu.vn, sglprdstudlab01.rmit.edu.vn, mytimetable.rmit.edu.vn, studentlab1.rmit.edu.vn, online-archived.rmit.edu.vn, and democlass.rmit.edu.vn. The 'Payload processing' section shows a table with columns 'Enabled' and 'Rule'.

Enabled	Rule

Để tránh bị coi là bruteforce vào tên miền này, ta sẽ cho delay các request bằng cách chọn Resource pool → tick vào ô delay between requests và nhập số ms mình muốn:

Sau khi chạy xong, ta lọc được request tới các subdomain sau đây có status code 200:

Request	Payload	Target	Status code ^	Response received
0		https://www.rmit.edu.vn	200	92
2	findaresearcher.rmit.edu.vn	https://findaresearcher.rmit.edu.vn	200	144
7	libtutorials.rmit.edu.vn	https://libtutorials.rmit.edu.vn	200	101
10	sglprdalumweb1.rmit.edu.vn	https://sglprdalumweb1.rmit.edu.vn	200	190
29	english.rmit.edu.vn	https://english.rmit.edu.vn	200	316
31	alumninetwork.rmit.edu.vn	https://alumninetwork.rmit.edu.vn	200	1012
33	sglprdstudlab01.rmit.edu.vn	https://sglprdstudlab01.rmit.edu.vn	200	144
35	studentlab1.rmit.edu.vn	https://studentlab1.rmit.edu.vn	200	155
37	democlass.rmit.edu.vn	https://democlass.rmit.edu.vn	200	171
38	experienceday.rmit.edu.vn	https://experienceday.rmit.edu.vn	200	201
48	helpdesk.rmit.edu.vn	https://helpdesk.rmit.edu.vn	200	204
72	sas.rmit.edu.vn	https://sas.rmit.edu.vn	200	313
75	pe.rmit.edu.vn	https://pe.rmit.edu.vn	200	787
76	omeka.rmit.edu.vn	https://omeka.rmit.edu.vn	200	366
90	design.rmit.edu.vn	https://design.rmit.edu.vn	200	558
92	chame.rmit.edu.vn	https://chame.rmit.edu.vn	200	107
95	etal.rmit.edu.vn	https://etal.rmit.edu.vn	200	600
99	learninglab.rmit.edu.vn	https://learninglab.rmit.edu.vn	200	1022
102	www.rmit.edu.vn	https://www.rmit.edu.vn	200	372
6	teachertalks.rmit.edu.vn	https://teachertalks.rmit.edu.vn	301	541

Như vậy, ta tìm được 18 subdomain trả về status code 200. Còn lại sẽ là các status code khác.

2. Host and Port Discovery

a) Tìm kiếm các host tương ứng

Bài tập 3: Ghi nhận lại các địa chỉ IP của tên miền phụ tìm được của

***.rmit.edu.vn. Kết quả lưu trong file csv**

Do ta đã tìm hơn 100 subdomain khác nhau của *.rmit.edu.vn nên để dễ dàng hơn cho việc tìm kiếm IP, ta sẽ sử dụng Shellsript.

Nội dung của Shellsript như sau:

```
(kali@kali)-[~]
$ cat rmit_ip.sh
#!/bin/bash

for i in $(cat 100rmitDomain.csv); do
    printf "%s\n" $(resolveip -s "$i") >> rmit_ip.csv
done
```

Shellsript này sẽ thực hiện việc lấy từng dòng của file 100rmitDomain.csv (file chứa các subdomain đã tìm được) và sử dụng công cụ resolveip để tìm IP của subdomain đó. Tất cả các kết quả sẽ được ghi thành từng dòng trong file "rmit_ip.csv".

Tiến hành chạy thử đoạn script trên và kiểm tra:

```
(kali@kali)-[~]
$ ./rmit_ip.sh
resolveip: Unable to find hostid for 'srs-docs.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'ocs-ng.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'pnt-wl-drweb5.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'dns2.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-wl-web5.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-wl-mekong2.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-aw-spydus01.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'password.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'pnt-wl-drweb3.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-wl-dls.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'online-archived.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'ave.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'careerhub.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'crm.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'dialin.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'election.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'ems.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'itop.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'lyncdiscover.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'mekong.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'mekong1.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'orsee.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-wl-web3.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sgs-ww-livesrv.rmit.edu.vn': host not found
resolveip: Unable to find hostid for 'sip.rmit.edu.vn': host not found

(kali@kali)-[~]
$ cat rmit_ip.csv
103.253.91.29
103.253.91.29
103.144.84.153
103.253.91.28
23.236.62.147
103.253.88.36
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
```

Sau đó dùng lệnh “paste” để nối 2 file này với nhau theo từng dòng.

Ta có kết quả cuối cùng:

```
(kali@kali)-[~]
$ paste 100rmitDomain.csv rmit_ip.csv > rmit_subdomain_ip.csv

(kali@kali)-[~]
$ cat rmit_subdomain_ip.csv
password-assistance.rmit.edu.vn 103.253.91.29
findaresearcher.rmit.edu.vn 103.253.91.29
sbcsprdap85.rmit.edu.vn 103.144.84.153
sbcsprdap81.rmit.edu.vn 103.253.91.28
srs-docs.rmit.edu.vn
teachertalks.rmit.edu.vn 23.236.62.147
libtutorials.rmit.edu.vn 103.253.88.36
sglprdrevrprx01.rmit.edu.vn 103.253.91.29
master-of-global-trade.rmit.edu.vn 171.244.39.11
sglprdalumweb1.rmit.edu.vn 103.253.91.24
ns1.rmit.edu.vn 103.253.91.22
ocs-ng.rmit.edu.vn
pnt-wl-drweb5.rmit.edu.vn
dns2.rmit.edu.vn
ns2.rmit.edu.vn 103.144.84.150
rmitlibraryvn.rmit.edu.vn 216.147.220.65
vpn.rmit.edu.vn 103.253.88.6
sgs-wl-web5.rmit.edu.vn
vpn2.rmit.edu.vn 103.253.88.4
sgs-wl-mekong2.rmit.edu.vn
sgs-aw-spydus01.rmit.edu.vn
```

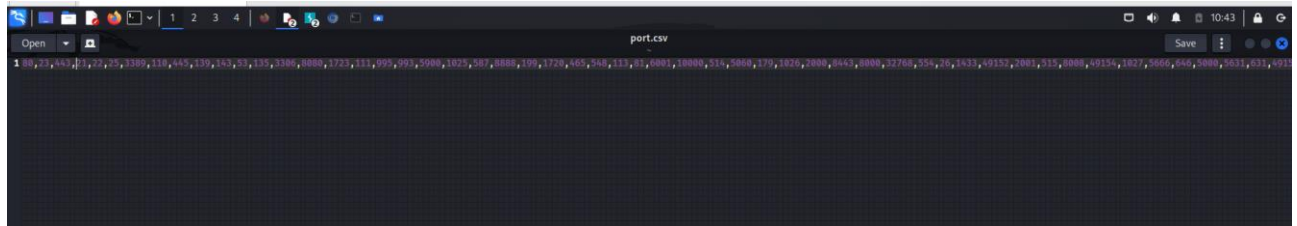
b) Tìm kiếm port tương ứng

Bài tập 4: Thực hiện scan 1000 port phổ biến trên các danh sách IP tìm được của *.rmit.edu.vn. Báo cáo kết quả tìm được trong file csv

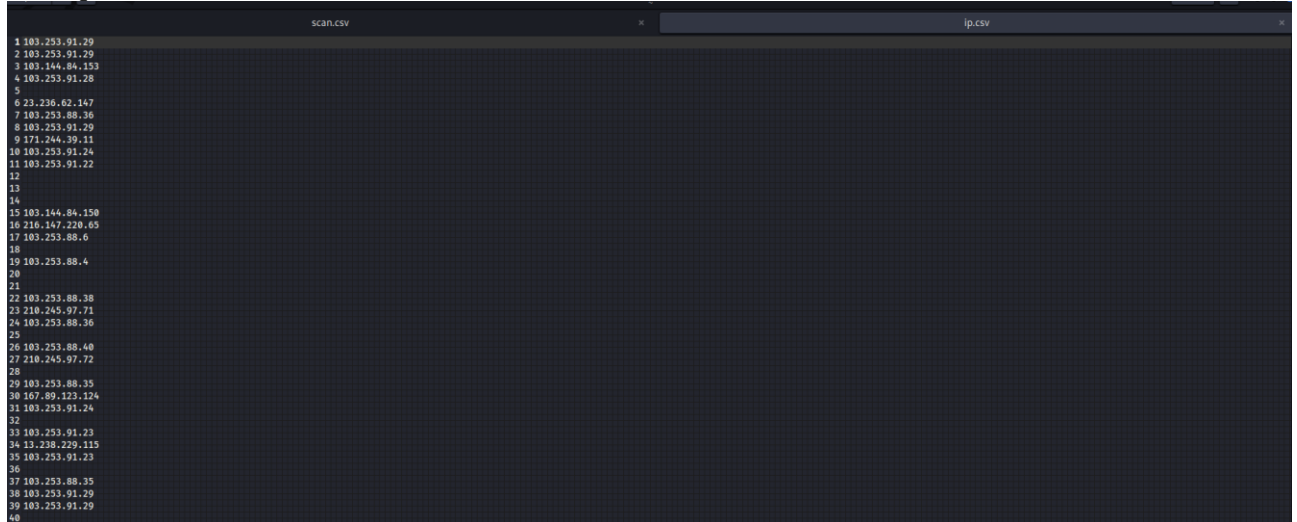
Dựa vào danh sách port đã được cung cấp

<https://raw.githubusercontent.com/HeckerBirb/top-nmap-ports-csv/master/top-1000-most-popular-tcp-ports-nmap-sorted.csv>

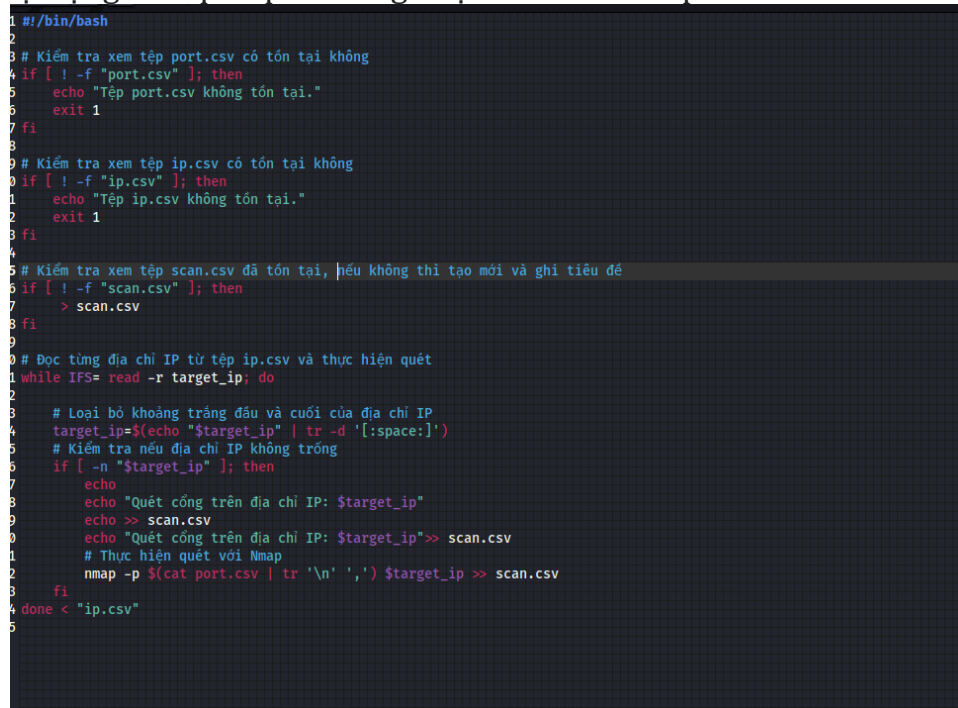
Trong danh sách có 2 port 1 và 1999 bị trùng lặp. Loại bỏ port trùng lặp và đưa vào file port.csv



File ip.csv đã có trước đó



Thực hiện tự động hóa quét port bằng đoạn mã bash script



Mục đích là đưa 2 file ip.csv và port.csv vào và sử dụng nmap để tự động quét file port cho mỗi địa chỉ IP

Cuối cùng là đưa output vào file scan.csv

Thực hiện đoạn bash script

```
(kali@kali)~[~]  
$ ./doccsv.sh ip.csv port.csv  
Quét cổng trên địa chỉ IP: 103.253.91.29  
Quét cổng trên địa chỉ IP: 103.253.91.29  
Quét cổng trên địa chỉ IP: 103.144.84.153  
Quét cổng trên địa chỉ IP: 103.253.91.28  
Quét cổng trên địa chỉ IP: 23.236.62.147  
Quét cổng trên địa chỉ IP: 103.253.88.36  
Quét cổng trên địa chỉ IP: 103.253.91.29  
Quét cổng trên địa chỉ IP: 171.244.39.11  
Quét cổng trên địa chỉ IP: 103.253.91.24  
Quét cổng trên địa chỉ IP: 103.253.91.22  
Quét cổng trên địa chỉ IP: 103.144.84.150  
Quét cổng trên địa chỉ IP: 216.147.220.65  
Quét cổng trên địa chỉ IP: 103.253.88.6  
Quét cổng trên địa chỉ IP: 103.253.88.4  
Quét cổng trên địa chỉ IP: 103.253.88.38  
Quét cổng trên địa chỉ IP: 210.245.97.71  
Quét cổng trên địa chỉ IP: 103.253.88.36  
Quét cổng trên địa chỉ IP: 103.253.88.40  
Quét cổng trên địa chỉ IP: 210.245.97.72  
Quét cổng trên địa chỉ IP: 103.253.88.35  
Quét cổng trên địa chỉ IP: 167.89.123.124  
Quét cổng trên địa chỉ IP: 103.253.91.24  
Quét cổng trên địa chỉ IP: 103.253.91.23
```

Sau khi chạy xong vào xem file scan.csv

Một phần kết quả của file scan.csv

```
Open scan.csv  
664 Nmap scan report for 103.253.91.29  
665 Host is up (0.0064s latency).  
666 Not shown: 995 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)  
667 PORT      STATE SERVICE  
668 80/tcp    open  http  
669 443/tcp   open  https  
670  
671 Nmap done: 1 IP address (1 host up) scanned in 129.30 seconds  
672  
673 Quét cổng trên địa chỉ IP: 173.203.204.123  
674 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 09:04 EDT  
675 Nmap scan report for cargocollective.com (173.203.204.123)  
676 Host is up (0.21s latency).  
677 Not shown: 992 filtered tcp ports (no-response)  
678 PORT      STATE SERVICE  
679 22/tcp    open  ssh  
680 25/tcp    open  smtp  
681 80/tcp    open  http  
682 443/tcp   open  https  
683 5666/tcp  open  nrpe  
684 10000/tcp open  snet-sensor-mgmt  
685  
686 Nmap done: 1 IP address (1 host up) scanned in 20.26 seconds  
687  
688 Quét cổng trên địa chỉ IP: 34.149.87.45  
689 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 09:04 EDT  
690 Nmap scan report for 45.87.149.34.bc.googleusercontent.com (34.149.87.45)  
691 Host is up (0.040s latency).  
692 Not shown: 996 filtered tcp ports (no-response)  
693 PORT      STATE SERVICE  
694 80/tcp    open  http  
695 443/tcp   open  https  
696  
697 Nmap done: 1 IP address (1 host up) scanned in 45.86 seconds  
698  
699 Quét cổng trên địa chỉ IP: 192.0.78.235  
700 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 09:05 EDT  
701 Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
702 Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds  
703  
704 Quét cổng trên địa chỉ IP: 192.0.78.12  
705 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 09:05 EDT  
706 Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
```

3. Truy tìm thông tin của website

a) Tìm kiếm thông qua Internet Archive

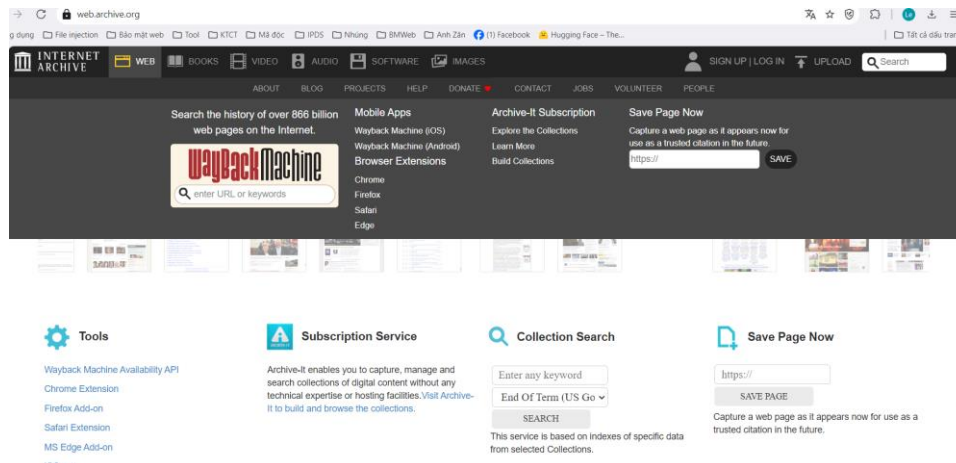
Internet Archive là một thư viện số phi lợi nhuận có trụ sở tại San Francisco, với sứ mệnh lưu trữ nội dung trên Internet. Một trong những dự án nổi tiếng của họ là Wayback Machine, một công cụ cho phép xem lại các phiên bản trang web từ quá khứ

Bài tập 5: Sử dụng <https://web.archive.org/> tìm kiếm và ghi nhận lại dữ liệu quá khứ các tên miền phụ không còn tồn tại hiện nay của *.rmit.edu.vn.

Khi tên miền phụ không còn hoạt động nó sẽ trả về status code 4xx

Thực hiện tìm kiếm thông qua Internet Archive

Giao diện:



Thực hiện tìm kiếm với các trang web
Srms.rmit.edu.vn 403

INTERNET ARCHIVE
Wayback Machine

Explore more than 866 billion web pages saved over time

[DONATE](#)

[Calendar](#) · [Collections](#) · [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

1 URL has been captured for this URL prefix.

Filter results by URL or MIME Type (i.e. '.txt')

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://rmit.edu.vn/dp-calendar	text/html	Sep 29, 2010	Sep 29, 2010	1	0	1

Showing 1 to 1 of 1 entries

First Previous **1** Next Last

[FAQ](#) | [Contact Us](#) | [Terms of Service \(Dec 31, 2014\)](#)

sgs-wl-omeka.rmit.edu.vn 403

[DONATE](#) **WayBack Machine** Explore more than 866 billion web pages saved over time

sgs-wi-omeka.rmit.edu.vn

[Calendar](#) · [Collections](#) · [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

No URL has been captured for this URL prefix.

MIME Type	From	To	Captures	Duplicat
No URLs				

Email.rmit.edu.vn

404

[DONATE](#) **WayBack Machine** Explore more than 866 billion web pages saved over time

Email.rmit.edu.vn

[Calendar](#) · [Collections](#) · [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

No URL has been captured for this URL prefix.

MIME Type	From	To	Captures	Duplicates
No URLs				

Mytimetable.rmit.edu.vn 410

[DONATE](#) **WayBack Machine** Explore more than 866 billion web pages saved over time

Mytimetable.rmit.edu.vn

[Calendar](#) · [Collections](#) · [Changes](#) · [Summary](#) · [Site Map](#) · [URLs](#)

8 URLs have been captured for this URL prefix.

Filter results by URL, or MIME Type (i.e., ".txt")

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
https://mytimetable.rmit.edu.vn/evn/mytimetable/	text/html	Jun 1, 2023	Jun 1, 2023	1	0	1
https://mytimetable.rmit.edu.vn/evn/mytimetable/css/concat.min.css	text/css	Apr 8, 2024	Apr 8, 2024	1	0	1
https://mytimetable.rmit.edu.vn/evn/mytimetable/css/mobile.min.css	text/css	Apr 8, 2024	Apr 8, 2024	1	0	1
https://mytimetable.rmit.edu.vn/evn/mytimetable/js/concat.min.js	text/javascript	Apr 8, 2024	Apr 8, 2024	1	0	1
https://mytimetable.rmit.edu.vn/odd/student	text/html	Oct 19, 2021	Oct 19, 2021	1	0	1
https://mytimetable.rmit.edu.vn/odd/mytimetable/	text/html	Oct 19, 2021	Jun 1, 2023	2	0	2
https://mytimetable.rmit.edu.vn/odd/mytimetable/css/concat.min.css	text/css	Apr 11, 2023	Apr 11, 2023	1	0	1
https://mytimetable.rmit.edu.vn/odd/mytimetable/css/mobile.min.css	text/css	Apr 11, 2023	Apr 11, 2023	1	0	1

Showing 1 to 8 of 8 entries

First Previous 1 Next Last

Careers.rmit.edu.vn

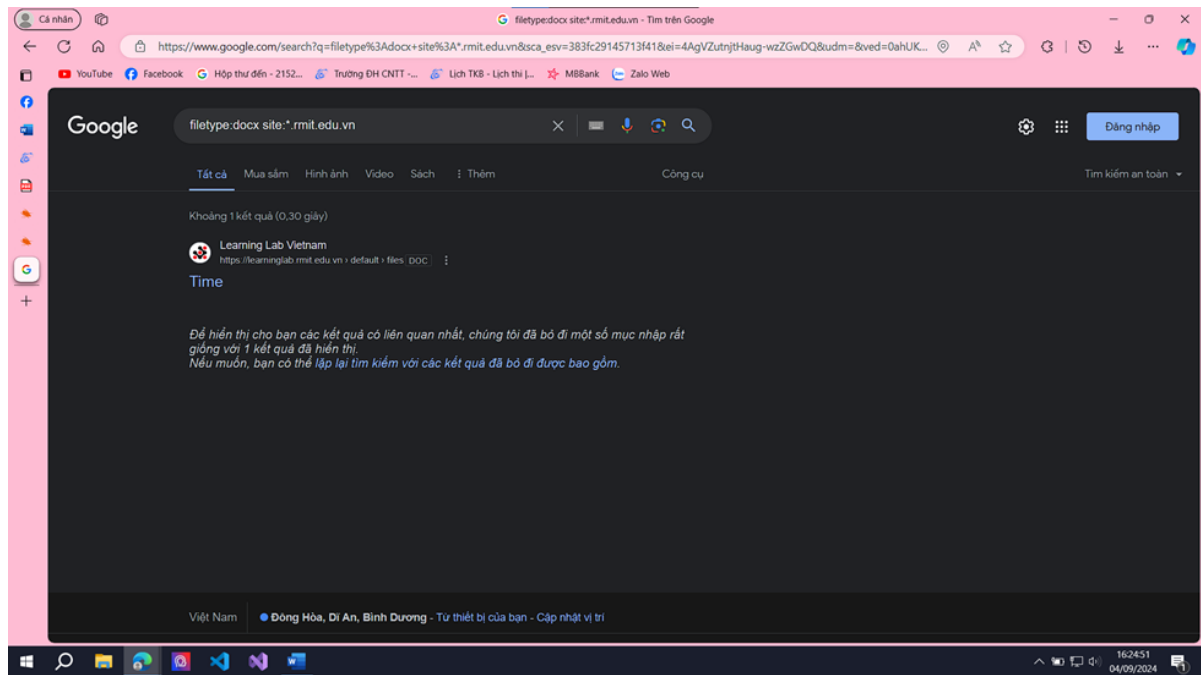
404

Emedia.rmit.edu.vn 403

[FAQ](#) | [Contact Us](#) | [Terms of Service](#) (Dec 31, 2014)

Bài tập 6: Tìm kiếm các tập tin pdf, excel, word, trên *.rmit.edu.vn.

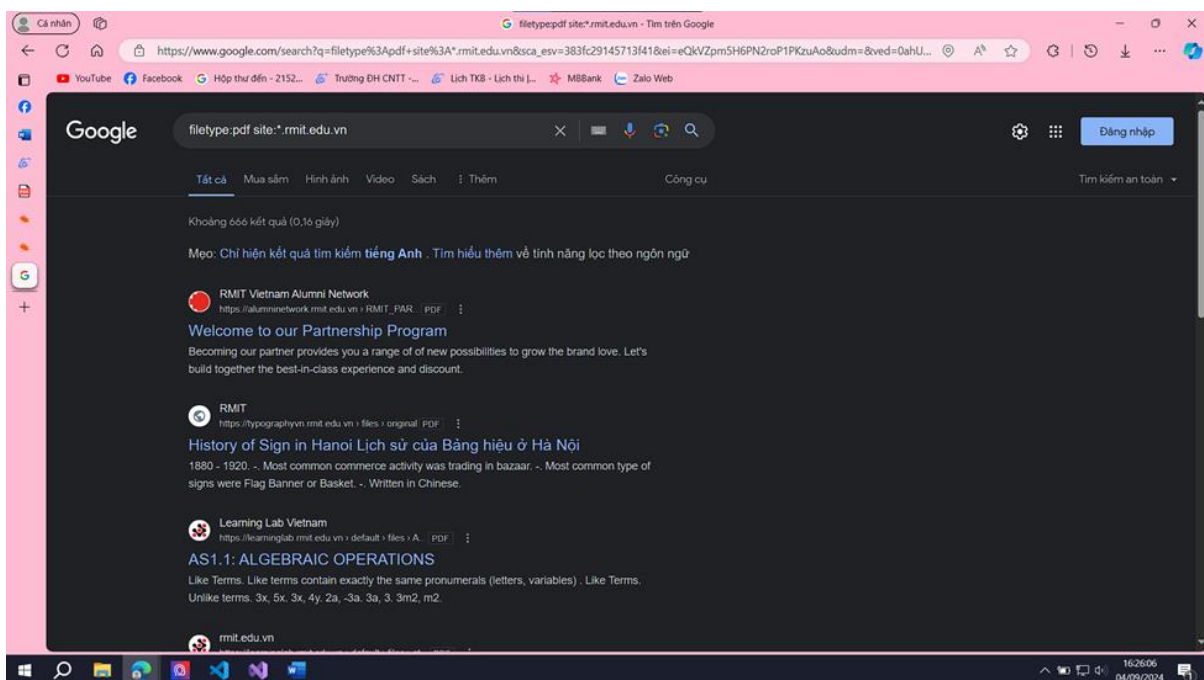
Kết quả



Tương tự cho các tập tin khác

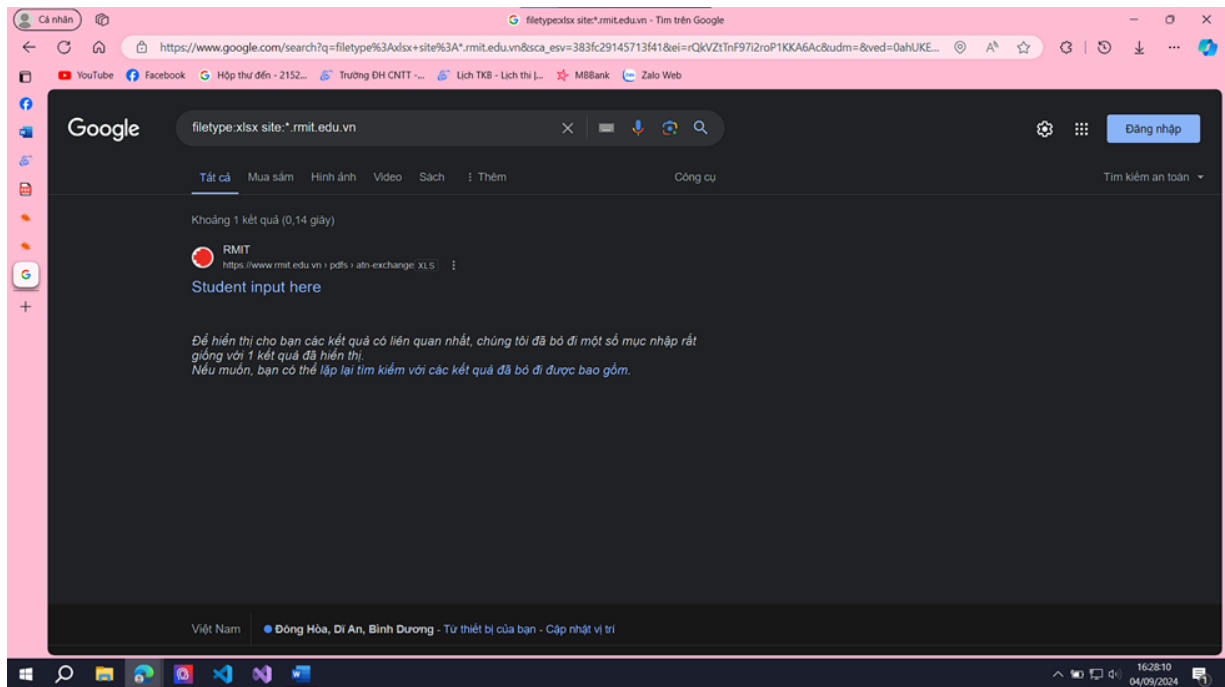
- Tập tin pdf: `filetype:pdf site:*.rmit.edu.vn`

Kết quả:



- Tập tin xlsx: `filetype:xlsx site:*.rmit.edu.vn`

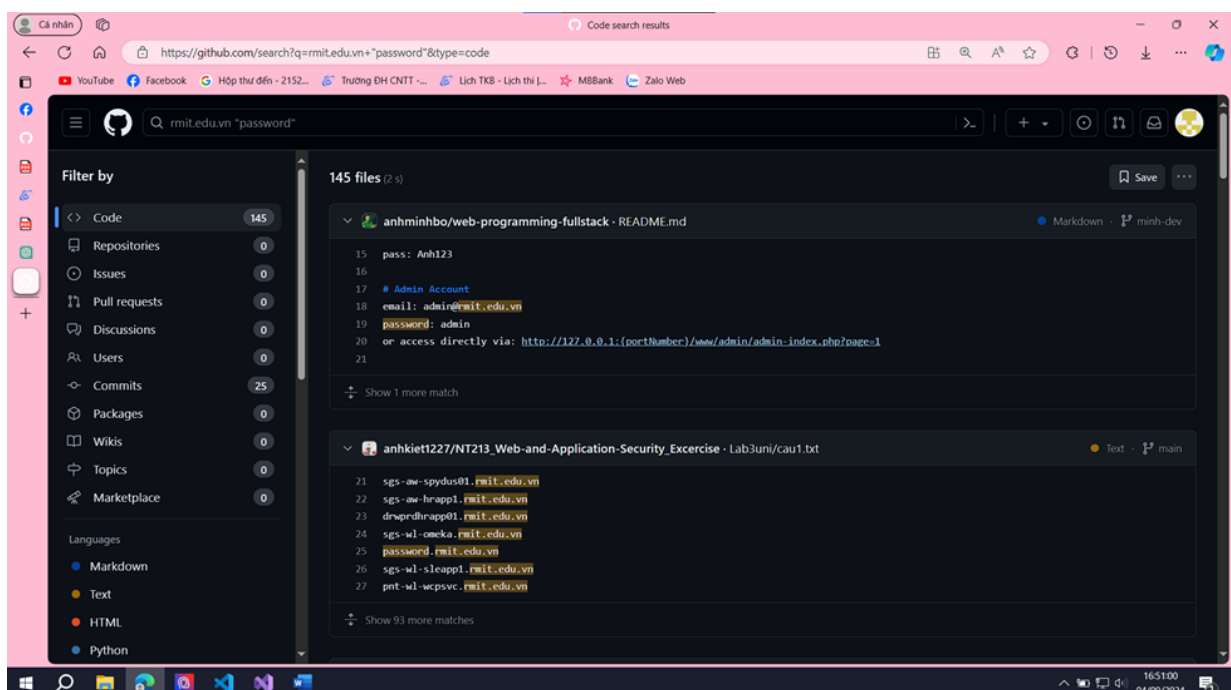
Kết quả:



c) Tìm kiếm thông qua github

Bài tập 7: Ghi nhận một vài thông tin tìm được trên github với domain *.rmit.edu.vn.

Thực hiện tìm kiếm trên github bằng phương pháp thủ công thì ta sẽ thực hiện bằng lệnh: `rmit.edu.vn "password"` chúng ta sẽ có được 1 số thông tin password có trong các phần code của 1 số cá nhân



Thực hiện tìm kiếm tự động:

Giao diện của công cụ

```
(kali㉿kali)-[~/Downloads/GitDorker]
$ python3 GitDorker.py -tf tf/TOKENSFILE -q rmit.edu.vn -d Dorks/medium_dorks.txt -o rmit

/$$$$$ /$ /$
/$$ _ $$|_ | $$
|$$_ \$/ $$/ $$$$$$
|$$_ /$$$| $$$ _ $$/
|$$_ _$$ $$_ $$_
|$$_ \$$ $$_ $$_ /$$
|$$$$$ /$ $$_ $$$/
\___/_ \___\___

/$$$$$$ /$
|$$_ _ $$
|$$_ \ $$ /$$$$$ /$$$$$
|$$_ | $$ /$$$ $$_ /$$_ $$$ /$$$ /$$$$$
|$$_ | $$ /$$$ $$_ /$$_ $$$ /$$$ /$$$ /$$$
|$$_ | $$ /$$$ $$_ /$$_ $$$ /$$$ /$$$ /$$$
|$$_ | $$ /$$$ $$_ /$$_ $$$ /$$$ /$$$ /$$$
|$$$$$ /$ $$$ /$$_ $$$
|$$$$$ /$ $$$ /$$_ $$$
\___/_ \___\___

Find GitHub secrets utilizing a vast list of GitHub dorks and the GitHub search api. The purpose of this tool is to enumerate interesting users, repos, and files to provide an easy to read overview of where a potential sensitive information exposure may reside.

HELP: python3 GitDorker.py -h

*****

[+] 0 organizations found.
[+] 0 users found.
[+] 240 dorks found.
[+] 0 keywords found.
[+] 1 queries ran.
[+] 240 urls generated.
[+] 1 tokens being used.
[+] running 1 threads.
[+] 29 requests per minute allowed
```

Thực hiện tìm kiếm với lệnh:

```
python3 GitDorker.py -tf tf/TOKENSFILE -q rmit.edu.vn -d Dorks/medium_dorks.txt -o  
rmit
```

Kết quả:

