BÁO CÁO THỰC HÀNH

**Bài thực hành số 03: Reconnaissance**

**Môn học:** Bảo mật Web và Ứng dụng

**Lớp:** NT213.P12.ANTT.1

**THÀNH VIÊN THỰC HIỆN (Nhóm xx):**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Phan Nguyễn Nhật Trâm | 22521501 |

|  |
| --- |
| **Điểm tự đánh giá** |
| **10** |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện | 4 ngày |
| Phân chia công việc |  |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

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

MỤC LỤC

[**A.** BÁO CÁO CHI TIẾT 2](#_Toc180398404)

[1. Subdomain Enumeration 2](#_Toc180398405)

[a. Liệt kê thông qua các nguồn trên internet 2](#_Toc180398406)

[b. Tìm kiếm chủ động tên miền thông qua kĩ thuật brute-force 3](#_Toc180398407)

[2. Host and Port Discovery 5](#_Toc180398408)

[a. Tìm kiếm các host tương ứng 5](#_Toc180398409)

[b. Tìm kiếm port tương ứng 6](#_Toc180398410)

[3. Truy tìm thông tin của website 8](#_Toc180398411)

[a. Tìm kiếm thông qua Internet Archive 8](#_Toc180398412)

[b. Tìm kiếm thông qua google dork 9](#_Toc180398413)

[c. Tìm kiếm thông qua github 10](#_Toc180398414)

[4. Bài tập thực hành 11](#_Toc180398415)

[a. Tìm kiếm các tên miền phụ của \*.uit.edu.vn 11](#_Toc180398416)

[b. Tìm kiếm các địa chỉ IP thuộc \*.uit.edu.vn và các cổng đang mở tương ứng 12](#_Toc180398417)

[c. Tìm kiếm các dữ liệu quá khứ của \*.uit.edu.vn 13](#_Toc180398418)

[d. Tìm kiếm các dữ liệu nhạy cảm của \*.uit.edu.vn thông qua google dork và github 13](#_Toc180398419)

# BÁO CÁO CHI TIẾT

## Subdomain Enumeration

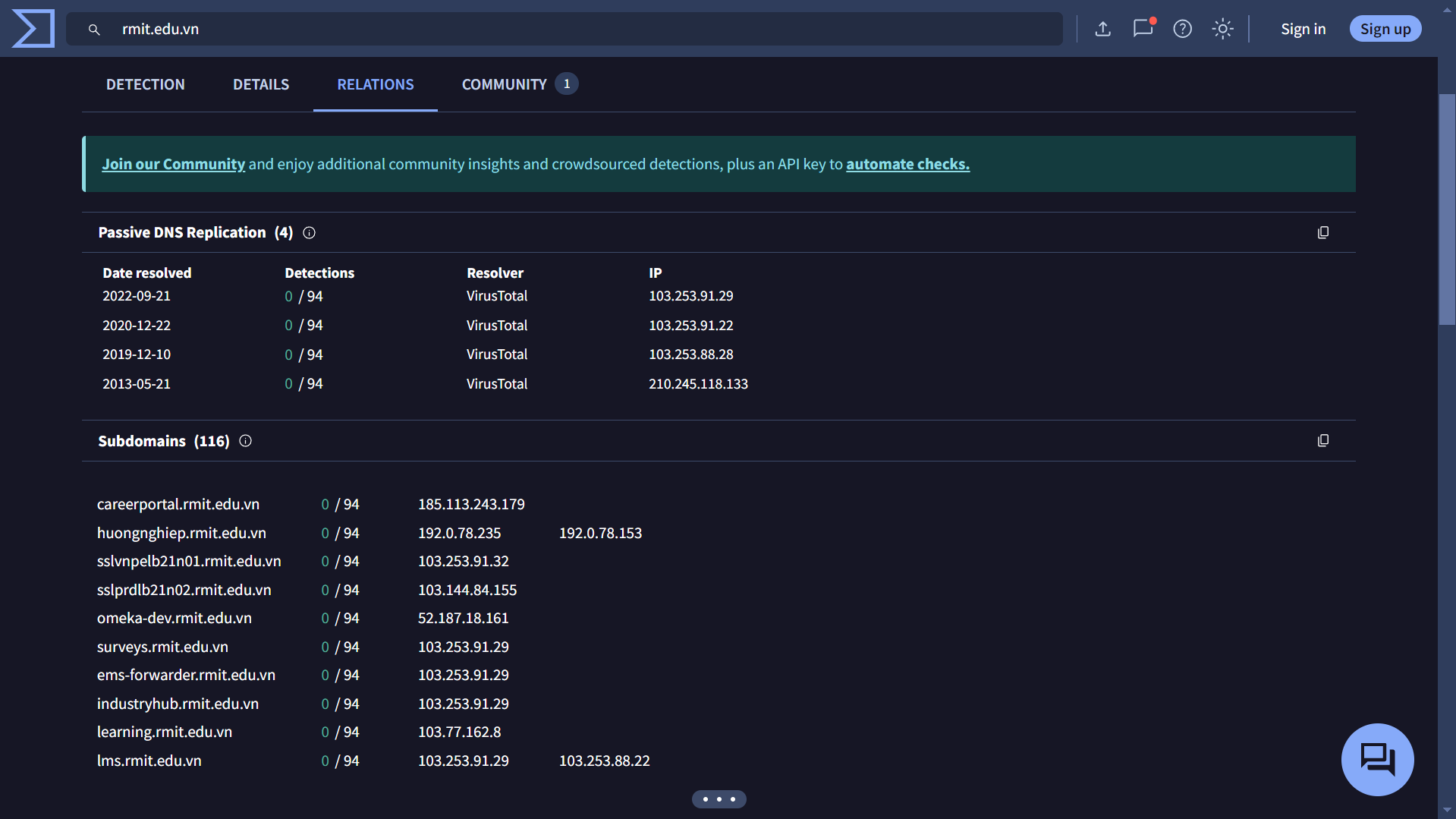
### Liệt kê thông qua các nguồn trên internet

Các nguồn có thể tìm kiếm dữ liệu công khai tên miền phụ ở đâu?

* VirusTotal
* Shodan
* Netcraft

Bài tập 1:

* Liệt kê ra ít nhất 100 tên miền phụ của rmit.edu.vn, kết quả được lưu trong file BaiTap1.csv.



1. Liệt kê miền phụ của rmit.uit.edu.vn bằng VirusTotal

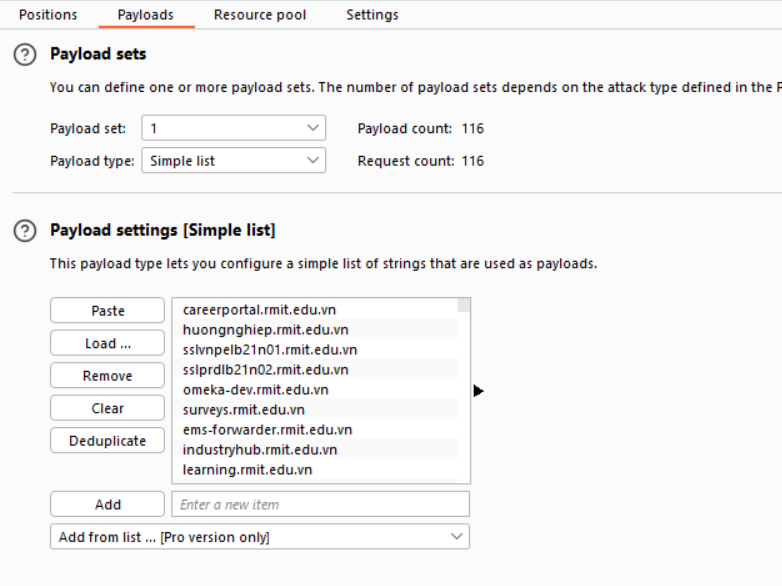
### Tìm kiếm chủ động tên miền thông qua kĩ thuật brute-force

Tập các danh sách tên miền phụ có thể tìm kiếm ở đâu và cách nào để đưa tên miền phụ vào burpsuite để tìm kiếm?

1. Bật Intercept On để chặn request
2. Đặt tải trọng tại *www.rmit.edu.vn*

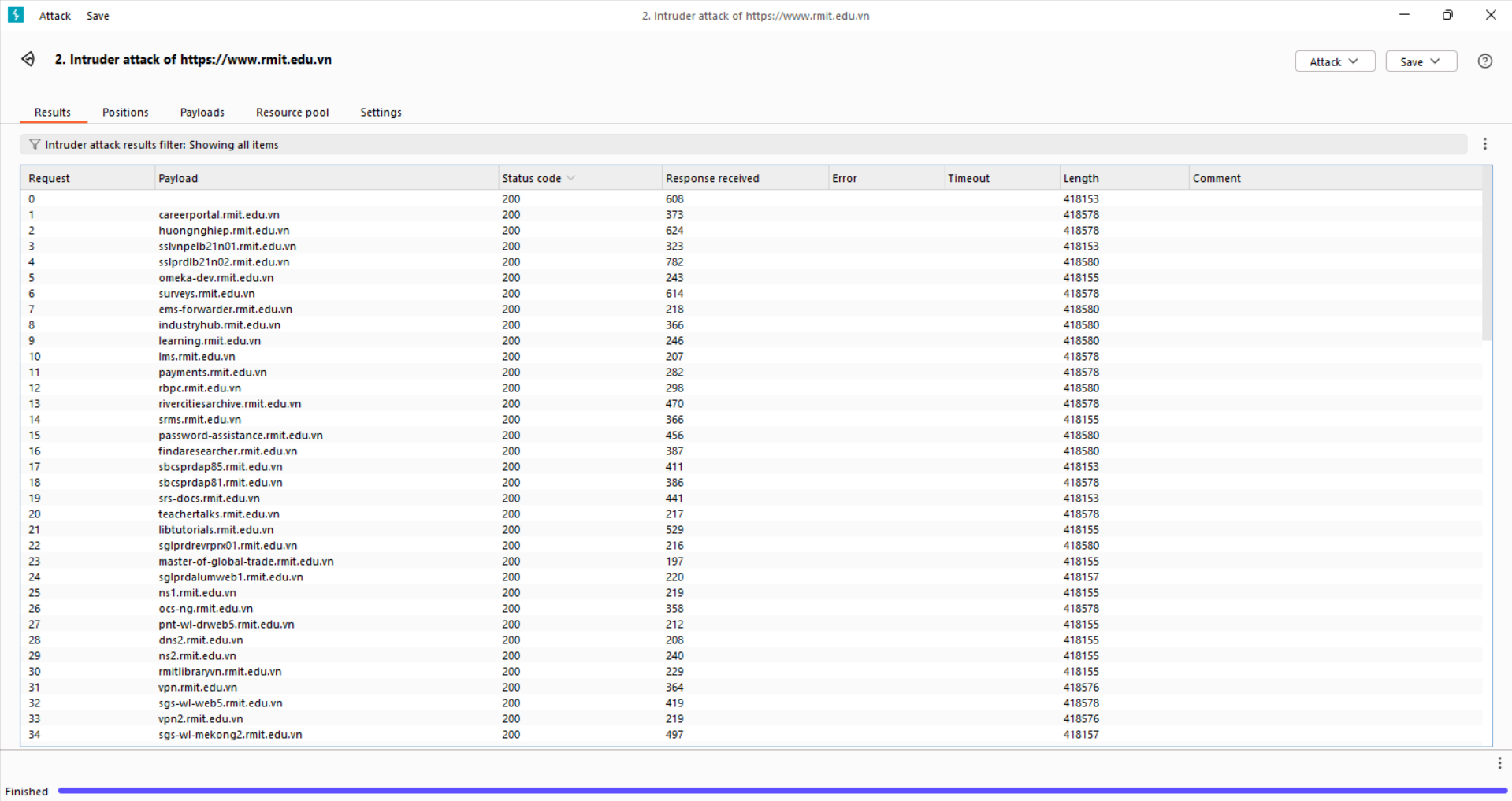


1. Đặt tải trọng để Brute-force
2. Trong Payload Options, chọn danh sách subdomain làm Payload Set



1. Đưa danh sách subdomain vào để tìm kiếm
2. Attack

Bài tập 2:



1. Kết quả trả về

## Host and Port Discovery

### Tìm kiếm các host tương ứng

Sử dụng cách nào để nhận được địa chỉ IP khi có được tên miền?

* nslookup
* ping

Bài tập 3:

* Với bài tập 3, ta viết một đoạn code python để lấy địa chỉ IP của từng subdomain đã tìm được ở bài tập 1 và 2
* Sử dụng thư viện socket của Python để lấy địa chỉ IP tương ứng với subdomain
* Nếu có subdomain không tìm thấy IP, ghi Not Found vào file BaiTap3.csv.

import socket

import csv

with open('BaiTap1.csv', 'r') as file:

subdomains = [line.strip() for line in file.readlines()]

with open('BaiTap3.csv', 'w', newline='') as csvfile:

fieldnames = ['Subdomain', 'IP Address']

writer = csv.DictWriter(csvfile, fieldnames=fieldnames)

writer.writeheader()

for subdomain in subdomains:

try:

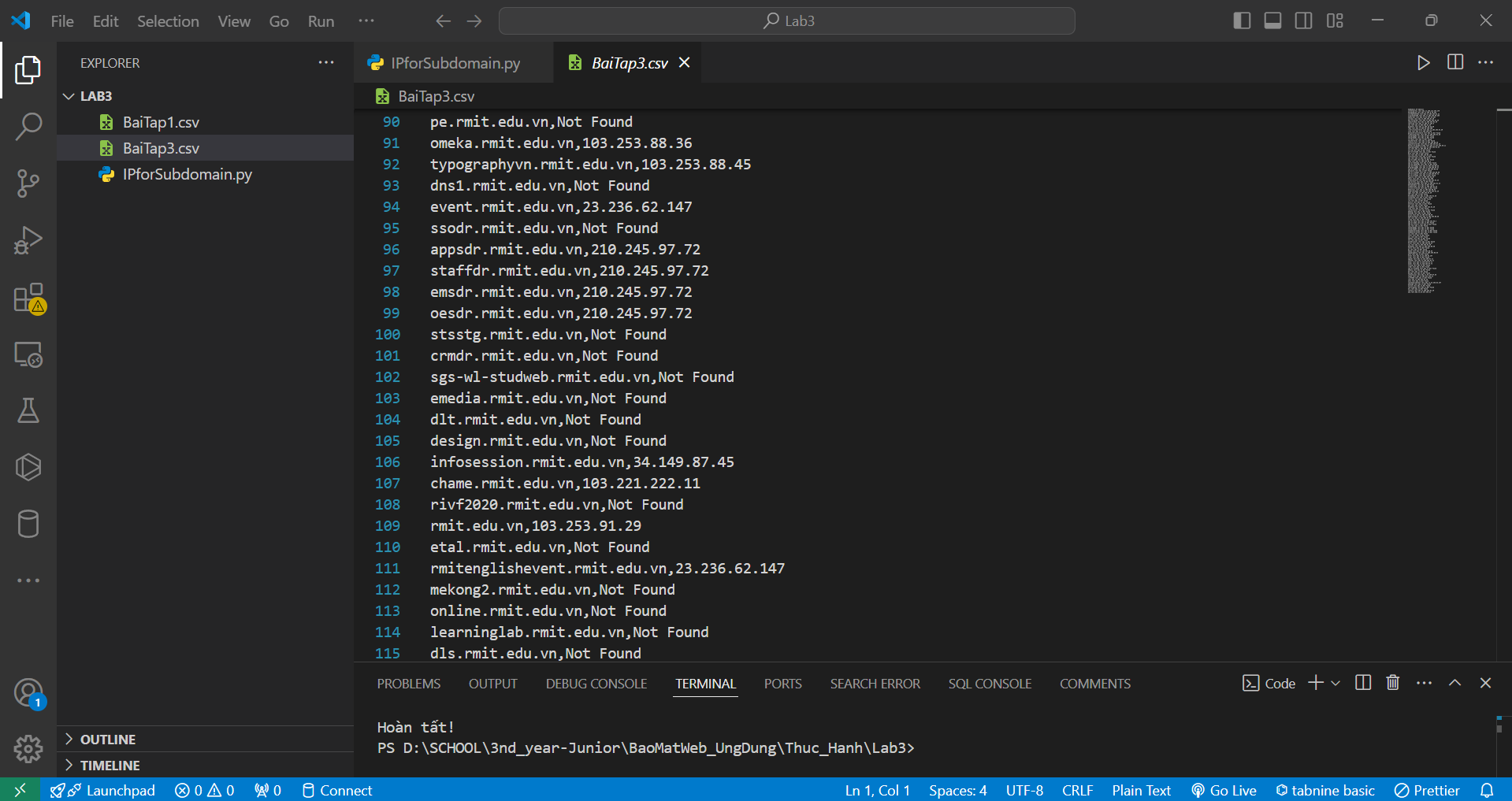
ip\_address = socket.gethostbyname(subdomain)

writer.writerow({'Subdomain': subdomain, 'IP Address': ip\_address})

except socket.gaierror:

writer.writerow({'Subdomain': subdomain, 'IP Address': 'Not Found'})

print("Hoàn tất!")



1. Kết quả lấy địa chỉ IP của các subdomain

### Tìm kiếm port tương ứng

Các công cụ scan port hiện nay có thể sử dụng là gì nmap, naabu, nessus, netcat ...?

* nmap
* netcat

Bài tập 4:

* Với bài tập 4, trước hết ta sửa đoạn code ở bài 3 để không cần ghi các ‘domain not found IP’
* Ta viết một đoạn code python để lấy port mở của từng IP đã tìm được ở bài tập 3
* Lệnh nmap được gọi thông qua subprocess.run, và kết quả được lưu vào stdout
* Kết quả đầu ra của nmap được tách thành từng dòng và kiểm tra xem dòng nào chứa port mở (/tcp và open). Nếu tìm thấy, các port sẽ được ghi vào file results.csv dưới dạng IP, open\_ports

import csv

import subprocess

ip\_file = 'IP.csv'

ports\_file = 'top-1000-most-popular-tcp-ports-nmap-sorted.csv'

output\_file = 'results.csv'

with open(ip\_file, 'r') as file:

ip\_list = [row[0] for row in csv.reader(file)]

with open(ports\_file, 'r') as file:

port\_list = file.read().strip()

with open(output\_file, 'w', newline='') as file:

writer = csv.writer(file)

writer.writerow(['IP', 'Open Ports'])

for ip in ip\_list:

print(f"Scanning {ip}...")

try:

result = subprocess.run(

['nmap', '-p', port\_list, '--open', ip],

stdout=subprocess.PIPE, stderr=subprocess.PIPE, text=True

)

open\_ports = []

for line in result.stdout.splitlines():

if "/tcp" in line and "open" in line:

port = line.split("/")[0]

open\_ports.append(port)

if open\_ports:

writer.writerow([ip, ', '.join(open\_ports)])

except Exception as e:

print(f"Error scanning {ip}: {e}")

print("Completed. Results saved to results.csv.")

**A screenshot of a computer

Description automatically generated**

1. Kết quả scan 1000 port phổ biến trên các danh các IP \*. rmit.edu.vn

**A black square with white text

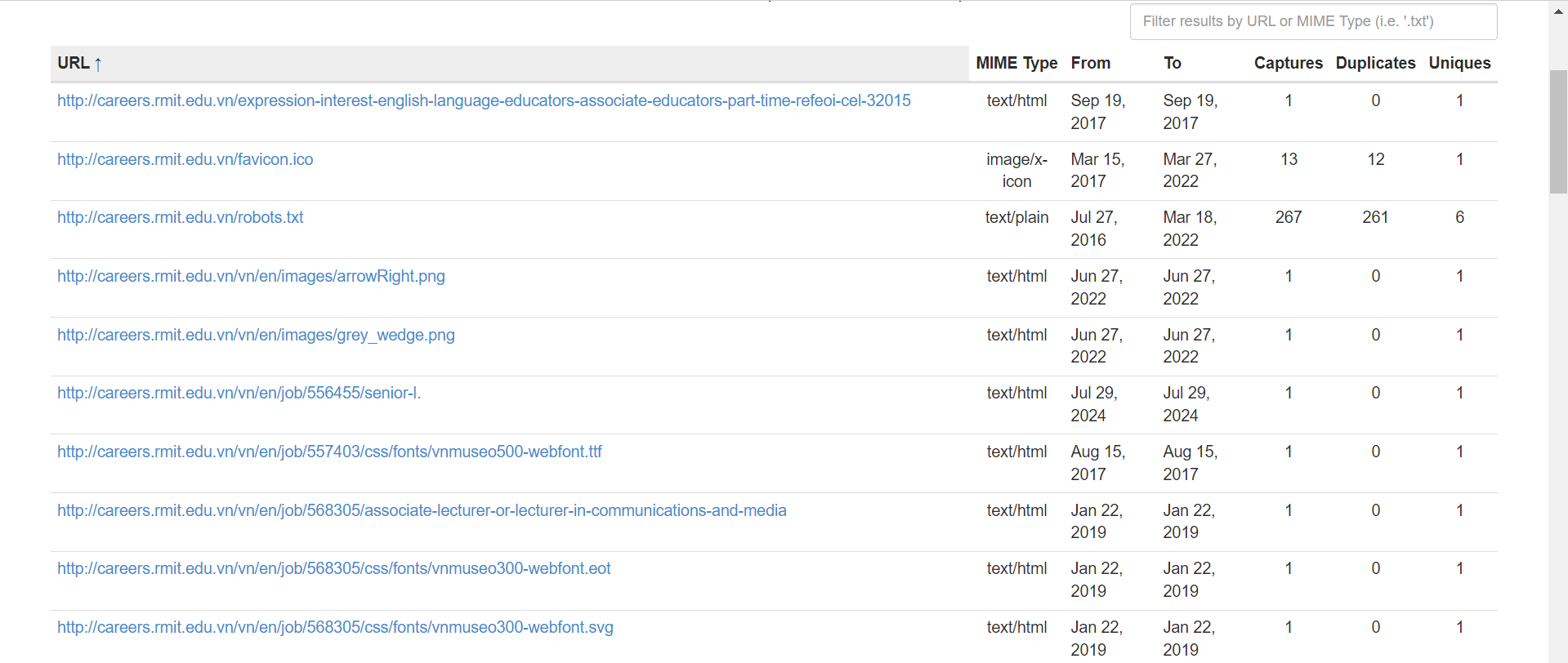
Description automatically generated with medium confidence**

1. Code chạy thành công

## Truy tìm thông tin của website

### Tìm kiếm thông qua Internet Archive

Bài tập 5:



1. careers.rmit.edu.vn

A screenshot of a computer

Description automatically generated

1. staff.rmit.edu.vn

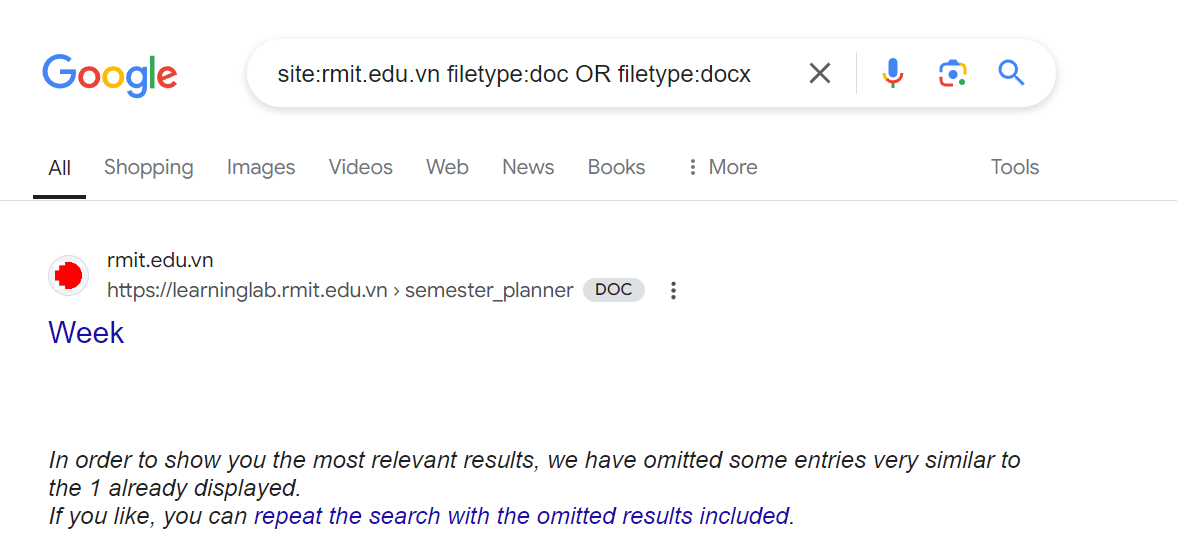
A screenshot of a computer

Description automatically generated

1. online.rmit.edu.vn

### Tìm kiếm thông qua google dork

Bài tập 6:



1. Tìm kiếm các tập tin word

A screenshot of a computer

Description automatically generated

1. Tìm kiếm các tập tin pdf

A screenshot of a computer

Description automatically generated

1. Tìm kiếm các tập tin excel

### Tìm kiếm thông qua github

Bài tập 7:

A screenshot of a computer

Description automatically generated

1. Sử dụng từ khóa api\_key để tìm kiếm thông tin nhạy cảm trên GitHub

A screenshot of a computer

Description automatically generated

1. Sử dụng từ khóa password để tìm kiếm thông tin nhạy cảm trên GitHub

## Bài tập thực hành

### Tìm kiếm các tên miền phụ của \*.uit.edu.vn

A screenshot of a computer

Description automatically generated

### Tìm kiếm các địa chỉ IP thuộc \*.uit.edu.vn và các cổng đang mở tương ứng

* Code

import socket

import csv

import nmap

with open('BT4a.csv', 'r') as file:

subdomains = [line.strip() for line in file.readlines()]

with open('BT4b.csv', 'w', newline='') as csvfile:

fieldnames = ['Subdomain', 'IP Address', 'Open Ports']

writer = csv.DictWriter(csvfile, fieldnames=fieldnames)

writer.writeheader()

nm = nmap.PortScanner()

for subdomain in subdomains:

try:

ip\_address = socket.gethostbyname(subdomain)

nm.scan(ip\_address, '1-1024') # Quét các cổng từ 1-1024

open\_ports = []

for proto in nm[ip\_address].all\_protocols():

ports = nm[ip\_address][proto].keys()

for port in ports:

if nm[ip\_address][proto][port]['state'] == 'open':

open\_ports.append(str(port))

writer.writerow({'Subdomain': subdomain, 'IP Address': ip\_address, 'Open Ports': ', '.join(open\_ports)})

except socket.gaierror:

continue

except Exception as e:

writer.writerow({'Subdomain': subdomain, 'IP Address': 'Error', 'Open Ports': str(e)})

print("Hoàn tất!")

* Kết quả



A screenshot of a computer

Description automatically generated

### Tìm kiếm các dữ liệu quá khứ của \*.uit.edu.vn

A screenshot of a computer

Description automatically generated

1. huongnghiep.uit.edu.vn

A screenshot of a computer

Description automatically generated

1. aiclub.uit.edu.vn

### Tìm kiếm các dữ liệu nhạy cảm của \*.uit.edu.vn thông qua google dork và github

* Google dork

A screenshot of a computer

Description automatically generated

1. Tìm kiếm các tập tin

* Github

A screenshot of a computer

Description automatically generated

1. Sử dụng từ khóa api\_key để tìm kiếm thông tin nhạy cảm trên GitHub