BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 3: Reconnaissance

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Võ Sỹ Minh	21521146	21521146@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá
1	**Chậm lại và suy nghĩ**	100%
2	**Bài tập 1**	100%
3	**Bài tập 2**	80%
4	**Bài tập 3**	100%
5	**Bài tập 4**	100%
6	**Bài tập 5**	100%
7	**Bài tập 6**	100%
8	**Bài tập 7**	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

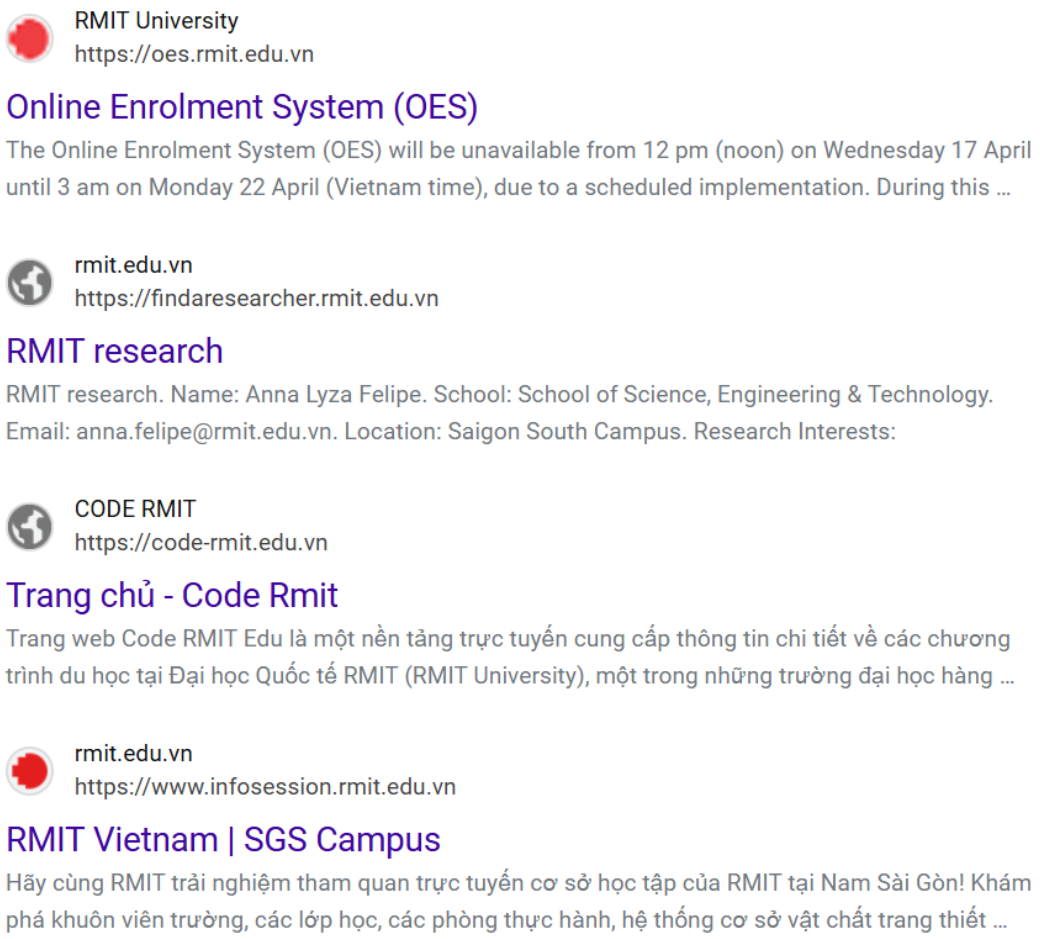
BÁO CÁO CHI TIẾT

Chậm lại và suy nghĩ 1: Các nguồn có thể tìm kiếm tên miền phụ ở đâu?

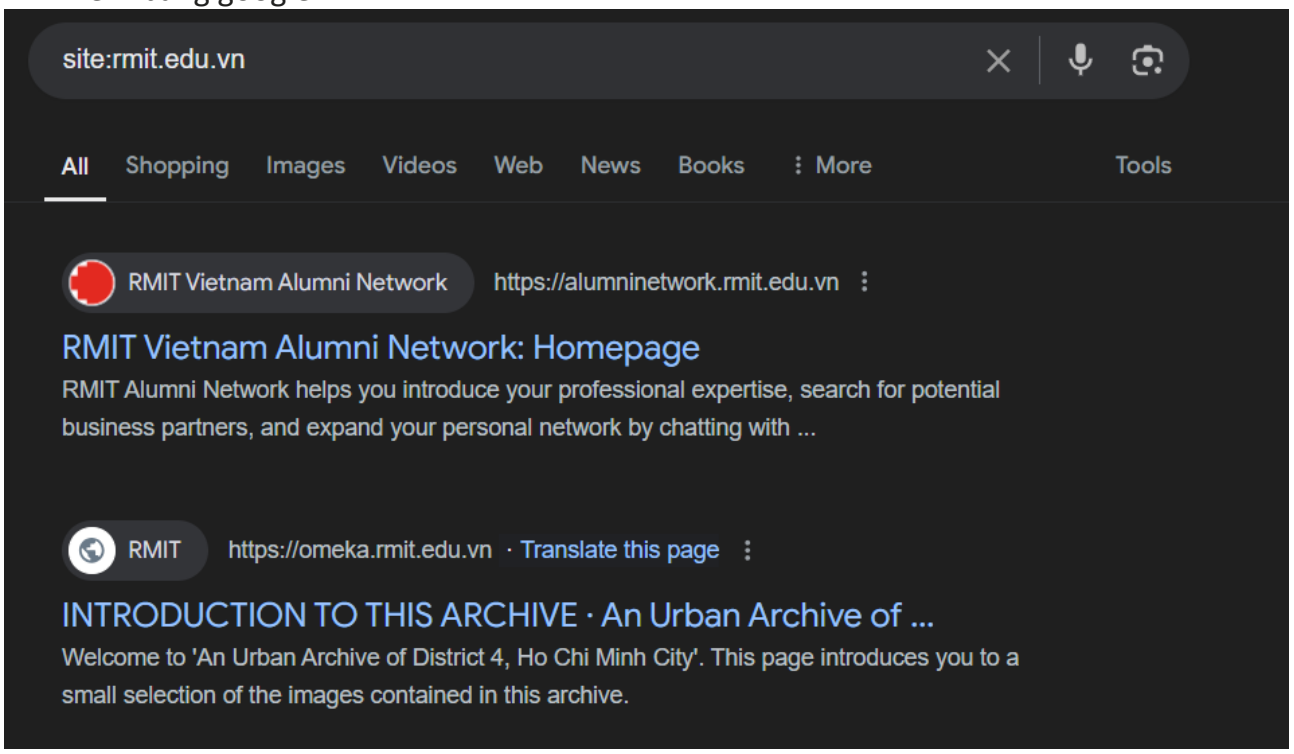
Có thể tìm ở những trình duyệt web như google, bing, baidu,... hoặc các trang web có tiện ích kèm theo như Virustotal, c99.nl, ...

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

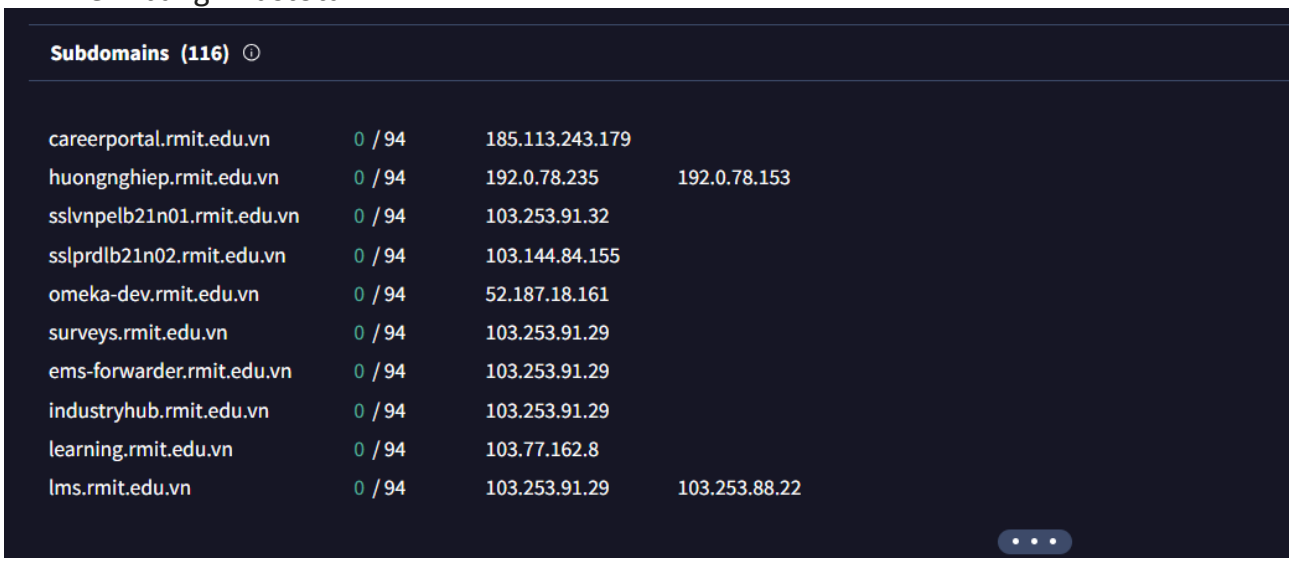
Tìm kiếm bằng bing:



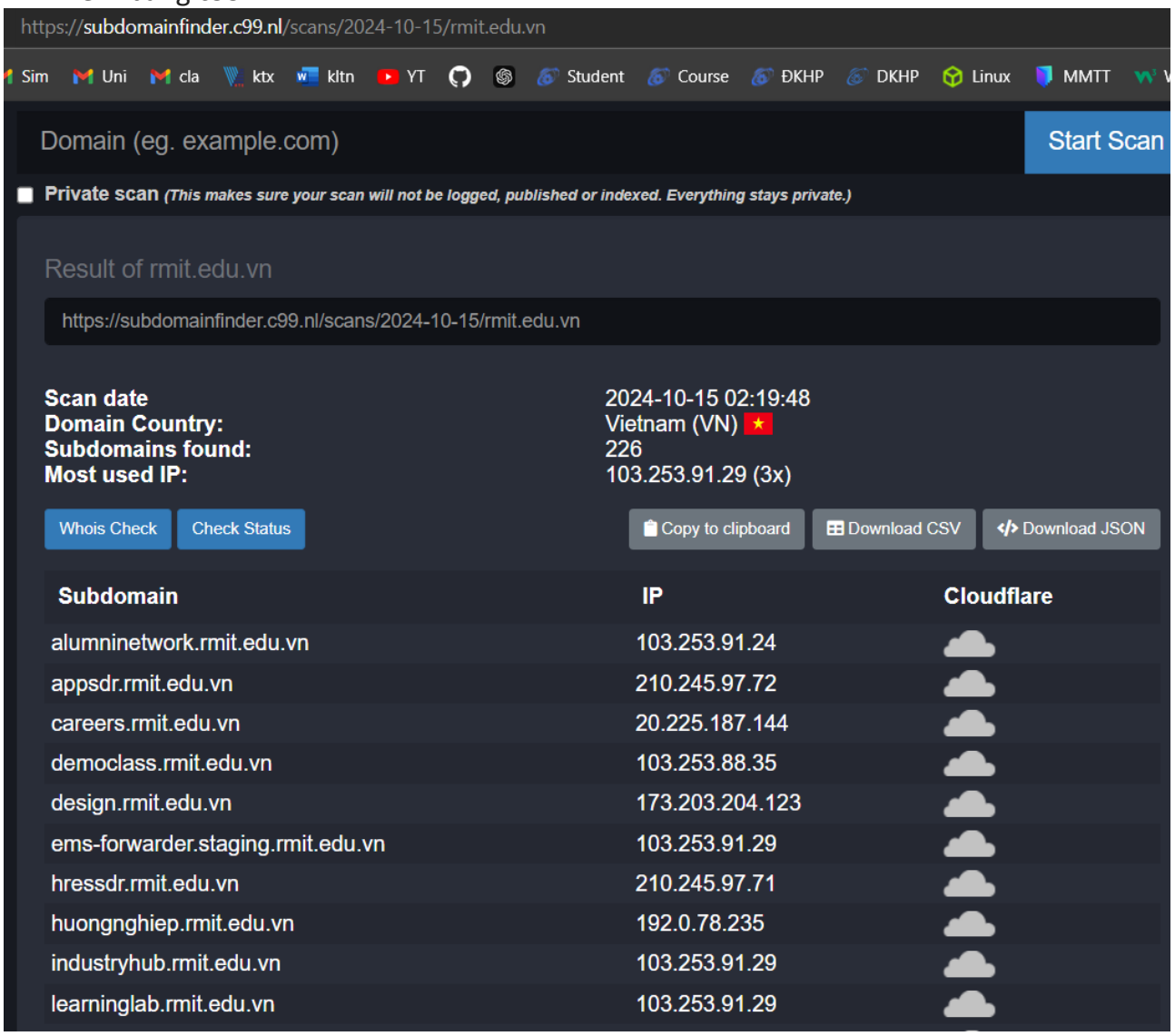
Tìm kiếm bằng google:



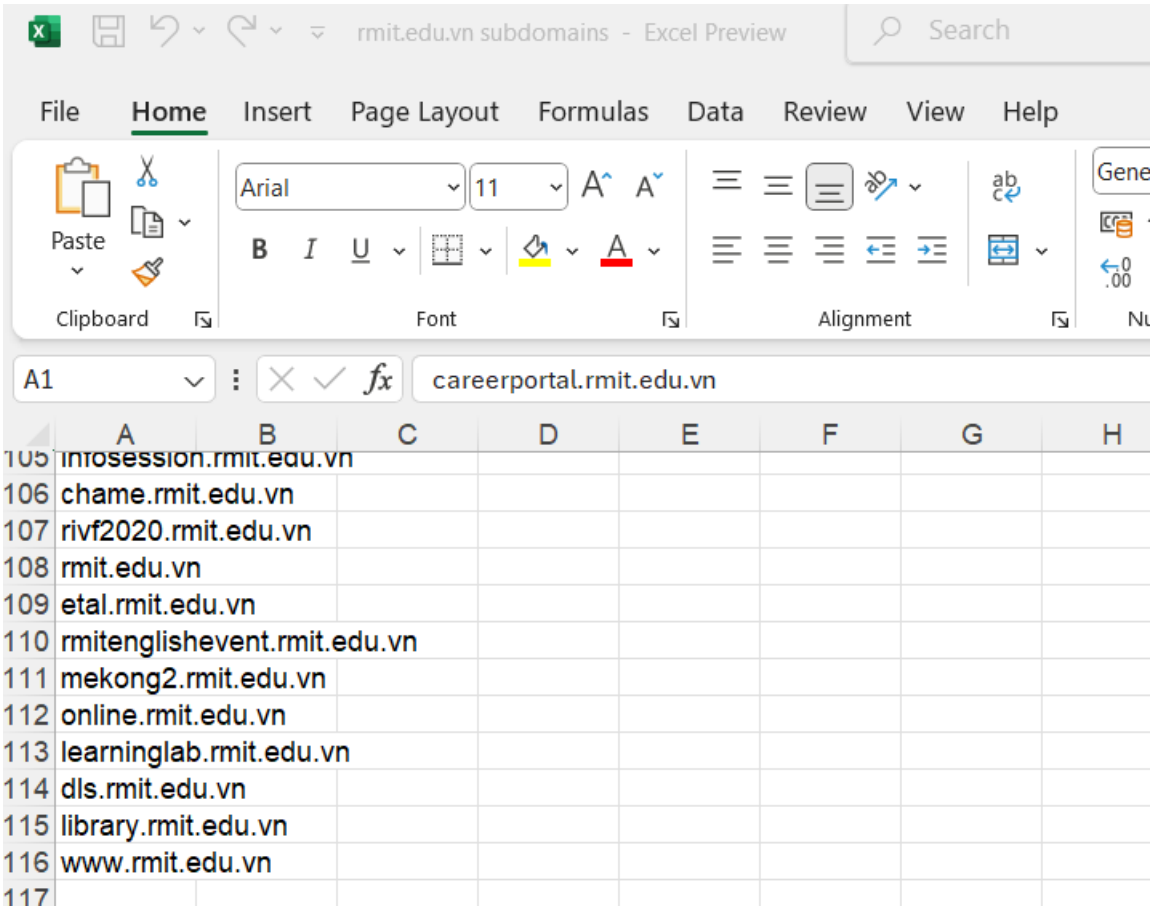
Tìm kiếm bằng virustotal:



Tìm kiếm bằng c99.nl:

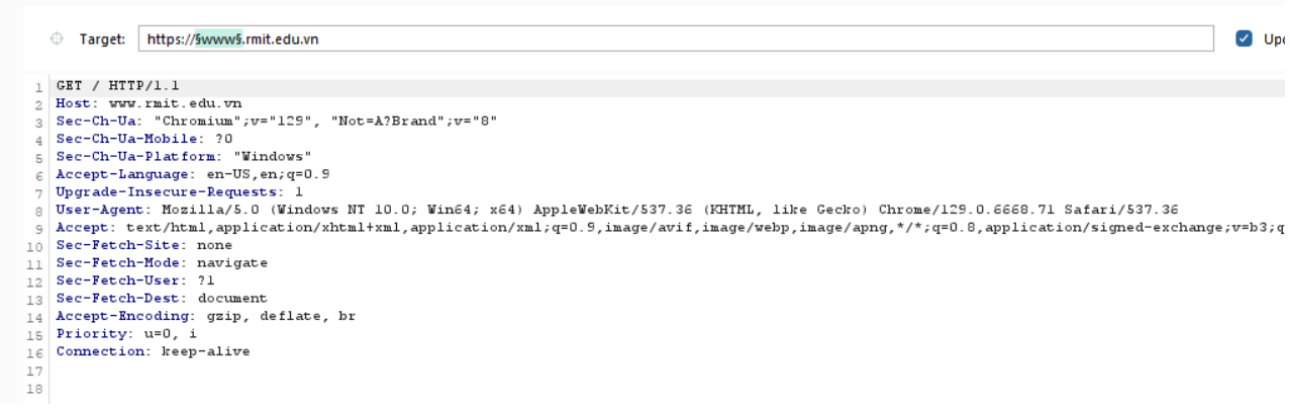


Lưu lại file rmit.edu.vn-subdomains.csv

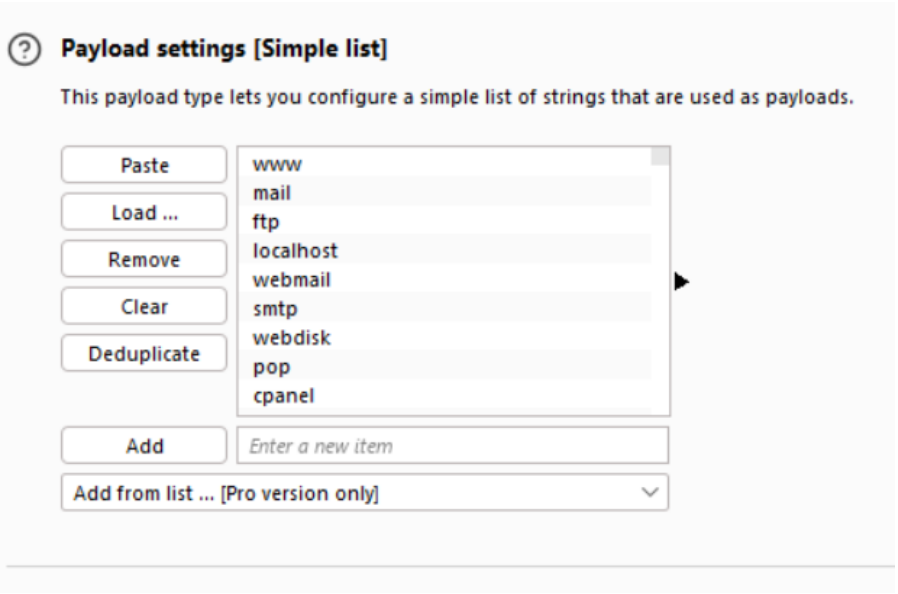


Chậm lại và suy nghĩ 2: Tập các danh sách tên miền phụ có thể tìm kiếm ở đâu và cách nào để đưa tên miền phụ và burpsuite để tìm kiếm?

Sử dụng option Intruder của burp suite để scan với payload list là subdomains-top1million-5000.txt
Biến sử dụng để quét subdomain:



Thêm payload.



Bắt đầu quét, các web khả dụng thì trả về status code như 200, 302, ...

Request	Payload	Target	Status code	Response received
0		https://www.rmit.edu.vn	200	431
1	huongnghiep	https://huongnghiep.rmit.edu.vn	200	704
2	www	https://www.rmit.edu.vn	200	315
101	helpdesk	https://helpdesk.rmit.edu.vn	200	295
88	apps	https://apps.rmit.edu.vn	302	175

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.

Sau 1 khoảng thời gian chạy, ta có được các tên miền có trả về kết quả status code 200 (trang web tương ứng tồn tại) và các tên miền có trả về kết quả khác như :
+ 301/302 (Redirect): Trang web được chuyển hướng đến một URL khác.
+ 403 (Forbidden): Truy cập vào trang web bị cấm.
+ 404 (Not Found): Trang web không tồn tại.
+ 500 (Internal Server Error): Lỗi máy chủ nội bộ.

Chậm lại và suy nghĩ 3: Sử dụng cách nào để nhận được địa chỉ IP khi có được tên miền?

Sử dụng công cụ nslookup:

```
> nslookup huongnghiep.rmit.edu.vn
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Server:  huongnghiep.rmit.edu.vn
Addresses:  192.0.78.153
          192.0.78.235
```

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.

```
┌──(simon㉿simon)-[~/Desktop/NT332-Lab01]
└─$ cat Ex3.sh
#!/bin/bash
for host in $(cat rmit_domain.txt); do
    printf "%s\n" $(resolveip -s "$host") >> rmitIP.txt
done


┌──(simon㉿simon)-[~/Desktop/NT332-Lab01]
└─$ ./Ex3.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
```

File rmitIP.txt có nhiều khoảng trống và IP trùng nên làm gọn file.

```
┌──(simon㉿simon)-[~/Desktop/NT332-Lab01]
└─$ grep -v '^$' rmitIP.txt | sort -u > temp.txt && mv temp.txt rmitIP.txt
```

Kết quả

```
 1 103.144.84.150
 2 103.144.84.153
 3 103.144.84.155
 4 103.221.222.11
 5 103.253.88.35
 6 103.253.88.36
 7 103.253.88.38
 8 103.253.88.4
 9 103.253.88.40
10 103.253.88.45
11 103.253.88.47
12 103.253.88.6
13 103.253.91.22
14 103.253.91.23
15 103.253.91.24
16 103.253.91.28
17 103.253.91.29
18 103.253.91.32
19 103.77.162.8
20 104.18.21.88
21 108.157.32.7
22 13.226.61.101
23 167.89.118.95
24 171.244.39.11
25 173.203.204.123
26 185.113.243.179
27 192.0.78.12
28 192.0.78.235
29 199.36.158.100
30 20.225.187.144
```

Chậm lại và suy nghĩ 4: Các công cụ scan port hiện nay có thể sử dụng là gì?

Nmap (Network Mapper): Là một trong những công cụ quét mạng và quét cổng phổ biến nhất. Nmap hỗ trợ nhiều kỹ thuật quét khác nhau, từ quét TCP, UDP, SYN cho đến quét stealth (ẩn danh). Nó cũng có thể phát hiện hệ điều hành và dịch vụ đang chạy trên các cổng được mở.

Masscan: Đây là công cụ quét cổng nhanh nhất hiện nay, có thể quét toàn bộ dải địa chỉ IPv4 trên thế giới chỉ trong vài phút. Masscan được sử dụng khi bạn cần tốc độ quét rất cao, tuy nhiên độ chính xác của nó có thể không cao bằng Nmap.

Netcat (NC): Ngoài khả năng quét cổng, Netcat còn có thể được sử dụng như một công cụ truyền dữ liệu hoặc mở các kết nối mạng đơn giản. Dù không mạnh mẽ như Nmap, Netcat rất linh hoạt và được sử dụng nhiều trong các bài kiểm tra bảo mật.

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.

File bash để scan IP:port và lưu vào

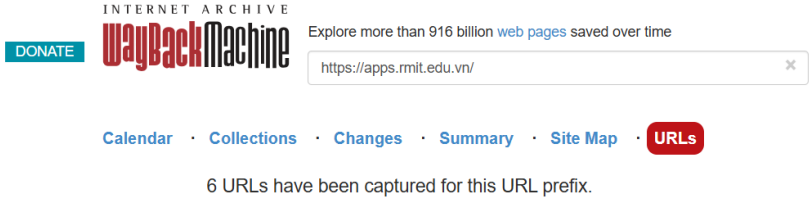
```
#!/bin/bash

# Đọc danh sách cổng từ file port.txt
ports=$(cat port.txt)

# Khởi tạo file CSV với tiêu đề
echo "IP,Port,State" > rmit_results.csv

# Duyệt qua từng IP trong rmitIP.txt và quét các cổng tương ứng
while IFS= read -r ip; do
    echo "Đang quét các cổng $ports cho IP: $ip"

    # Chạy nmap và trích xuất kết quả cổng và trạng thái
    nmap -p "$ports" "$ip" | grep 'open\|closed\|filtered' | while read -r line; do
        port=$(echo "$line" | awk '{print $1}' | cut -d'/' -f1)    # Lấy số cổng
        state=$(echo "$line" | awk '{print $2}')                   # Lấy trạng thái (open, closed, filtere
d)
        echo "$ip,$port,$state" >> rmit_results.csv                # Lưu vào file CSV
    done

done < rmitIP.txt
```

Kết quả có dạng sau

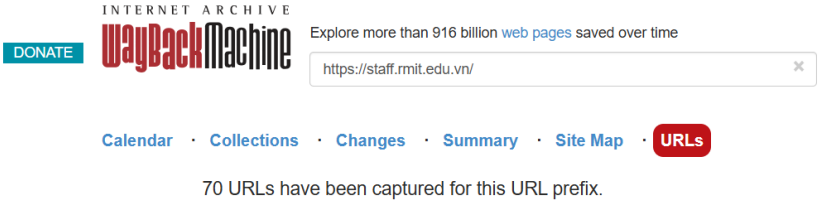
```
IP,Port,State
103.221.222.11,Not,shown:
103.221.222.11,21,open
103.221.222.11,80,open
103.221.222.11,110,open
103.221.222.11,143,open
103.221.222.11,443,open
103.221.222.11,465,open
103.221.222.11,587,open
103.221.222.11,993,open
103.221.222.11,995,open
103.221.222.11,3306,open
103.253.88.35,Not,shown:
103.253.88.35,80,open
```

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

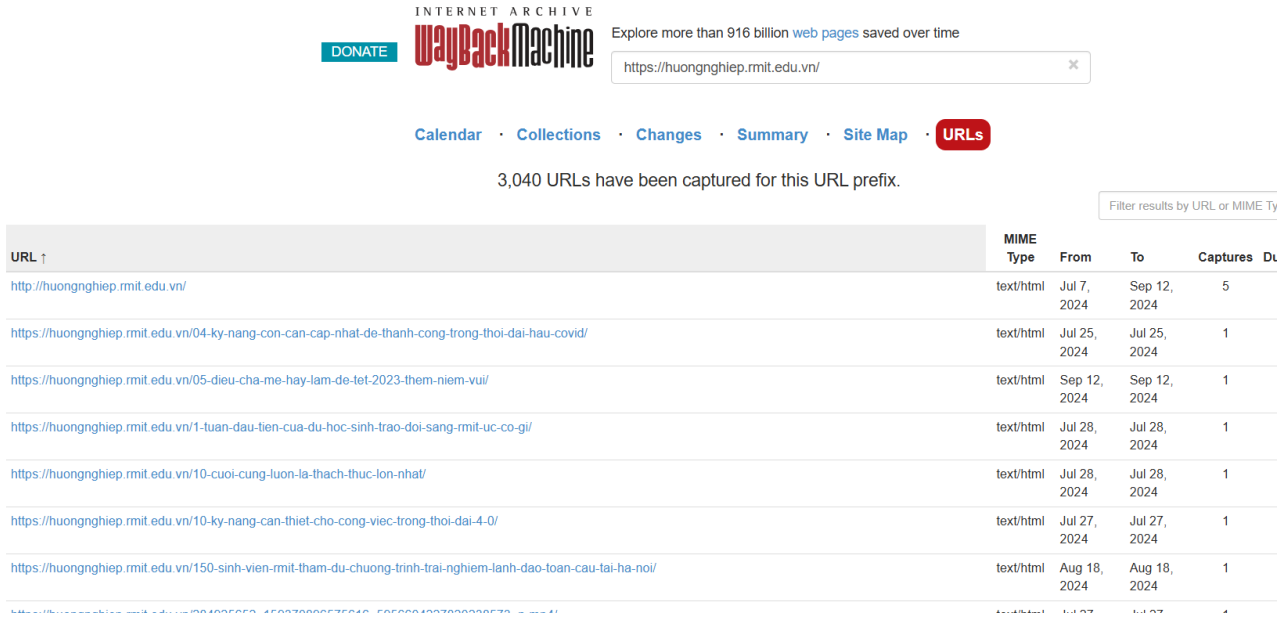
Thử tìm kiếm để xem các hoạt động với các subdomain như apps, staff, huongnghiep,...



URL ↑	MIME Type	From	To	Captures
http://apps.rmit.edu.vn/	text/html	Apr 19, 2023	Jun 17, 2024	4
https://apps.rmit.edu.vn/favicon.ico	image/vnd.microsoft.icon	Apr 19, 2023	Apr 19, 2023	1
https://apps.rmit.edu.vn/robots.txt	text/plain	Jun 4, 2018	Jun 21, 2018	4
https://apps.rmit.edu.vn/saml/discovery	text/html	Apr 19, 2023	Apr 19, 2023	1
https://apps.rmit.edu.vn/saml/login	text/html	Apr 19, 2023	Apr 19, 2023	1
https://apps.rmit.edu.vn/saml/login?idp=https%3A//myapps.rmit.edu.au/nidp/saml2/metadata	text/html	Apr 19, 2023	Apr 19, 2023	1



URL ↑	MIME Type	From	To	Captures
https://staff.rmit.edu.vn/	text/html	Jun 21, 2020	Aug 30, 2022	9
https://staff.rmit.edu.vn/favicon.ico	image/vnd.microsoft.icon	Apr 29, 2016	Jan 8, 2022	5
https://staff.rmit.edu.vn/misc/drupal.js	warc/revisit	Jan 22, 2019	Jan 22, 2019	1
https://staff.rmit.edu.vn/misc/drupal.js?pbdyeq	warc/revisit	Jan 22, 2019	Jan 22, 2019	1
https://staff.rmit.edu.vn/misc/jquery.js	warc/revisit	Jan 22, 2019	Jan 22, 2019	1
https://staff.rmit.edu.vn/misc/jquery.js?v=1.4.4	warc/revisit	Jan 22, 2019	Jan 22, 2019	1
https://staff.rmit.edu.vn/misc/jquery.once.js	warc/revisit	Jan 22, 2019	Jan 22, 2019	1
https://staff.rmit.edu.vn/misc/jquery.once.js?v=1.2	warc/revisit	Jan 22, 2019	Jan 22, 2019	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.css?pbdyeq	warc/revisit	Jan 22, 2019	Jan 22, 2019	1
https://staff.rmit.edu.vn/misc/ui/jquery.ui.button.min.js?v=1.8.7	warc/revisit	Jan 22, 2019	Jan 22, 2019	1

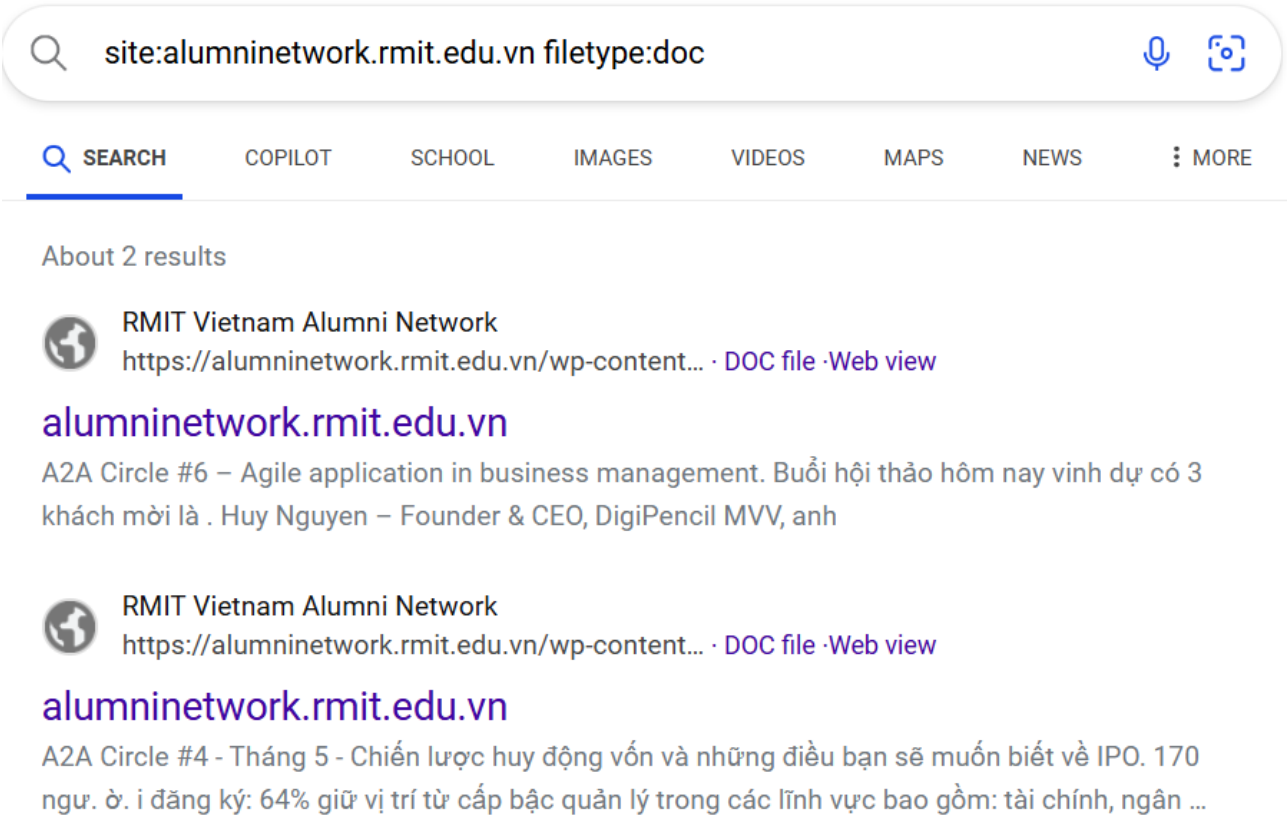


URL ↑	MIME Type	From	To	Captures	Du
http://huongnghiep.rmit.edu.vn/	text/html	Jul 7, 2024	Sep 12, 2024	5	
https://huongnghiep.rmit.edu.vn/04-ky-nang-con-can-cap-nhat-de-thanh-cong-trong-thoi-dai-hau-covid/	text/html	Jul 25, 2024	Jul 25, 2024	1	
https://huongnghiep.rmit.edu.vn/05-dieu-cha-me-hay-lam-de-tet-2023-them-niem-vui/	text/html	Sep 12, 2024	Sep 12, 2024	1	
https://huongnghiep.rmit.edu.vn/1-tuan-dau-tien-cua-du-hoc-sinh-trao-doi-sang-rmit-uc-co-gi/	text/html	Jul 28, 2024	Jul 28, 2024	1	
https://huongnghiep.rmit.edu.vn/10-cuoi-cung-luon-la-thach-thuc-lon-nhat/	text/html	Jul 28, 2024	Jul 28, 2024	1	
https://huongnghiep.rmit.edu.vn/10-ky-nang-can-thiet-cho-cong-viec-trong-thoi-dai-4-0/	text/html	Jul 27, 2024	Jul 27, 2024	1	
https://huongnghiep.rmit.edu.vn/150-sinh-vien-rmit-tham-du-chuong-trinh-trai-nghiem-lanh-dao-toan-cau-tai-ha-noi/	text/html	Aug 18, 2024	Aug 18, 2024	1	

Subdomain như staff đã có dấu hiệu của dừng hoạt động, còn apps và huongnghiep thì vẫn được capture đến năm 2024.

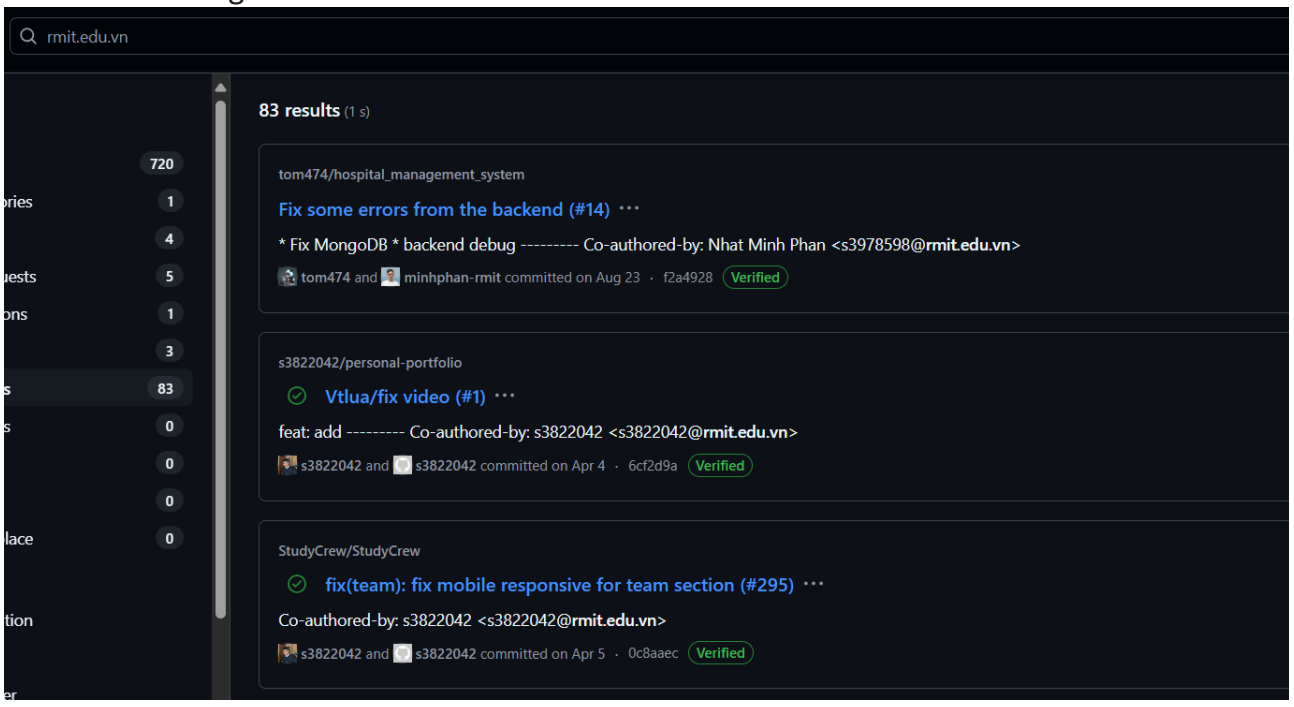
Bài tập 6: Tìm kiếm các tập tin pdf, excel, word, trên *.rmit.edu.vn.

Tìm kiếm với cấu trúc: site:*.rmit.edu.vn filetype:<type>
Ví dụ: site:alumninetwork.rmit.edu.vn filetype:doc
Hoặc kết hợp với OR : site:alumninetwork.rmit.edu.vn filetype:doc OR filetype:excel

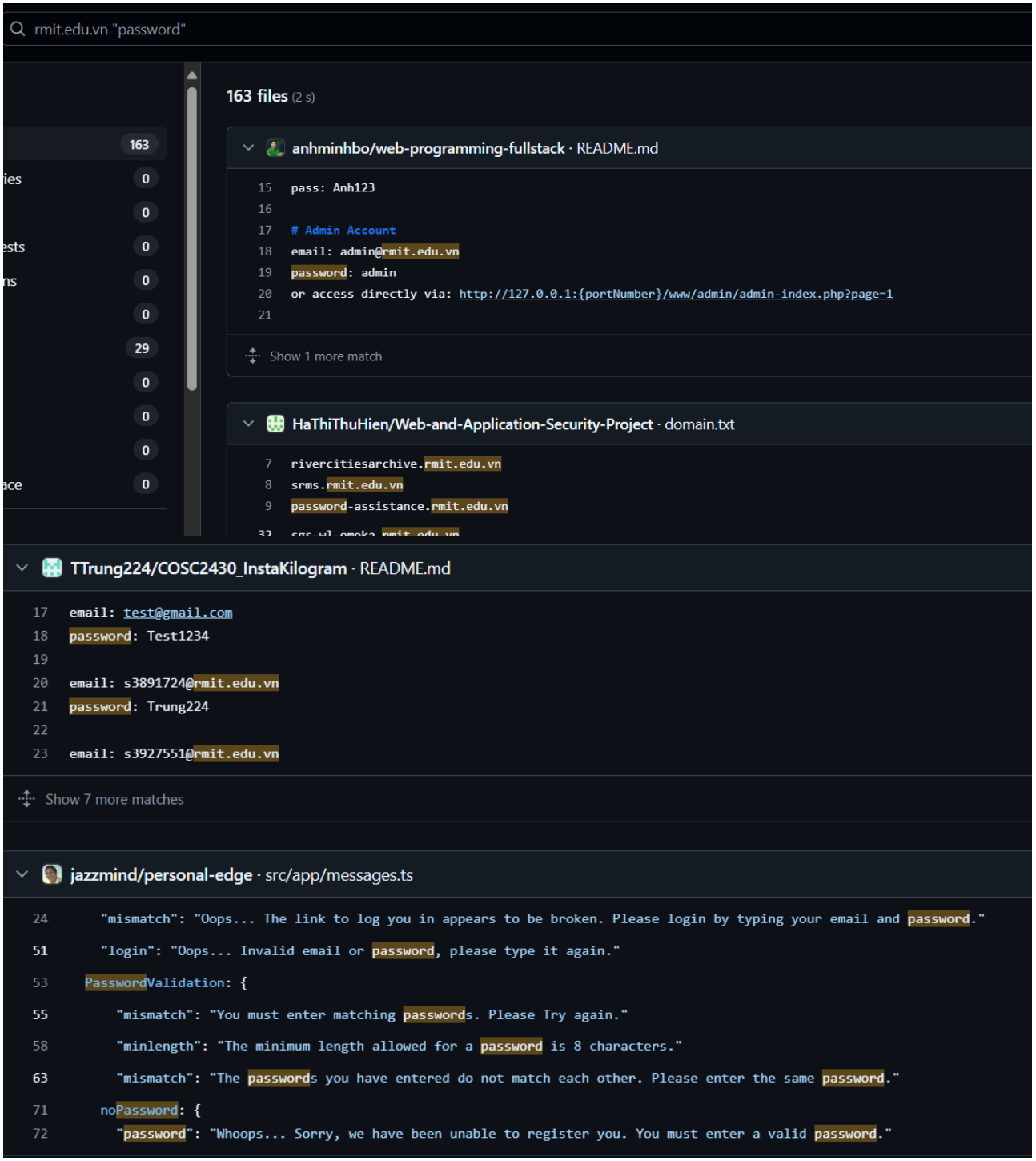


Bài tập 7: Ghi nhận một vài thông tin tìm được trên github với domain *.rmit.edu.vn

Các commit công khai



Kèm thêm chuỗi “password”



Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, 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 .DOCX và .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]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- 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 bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT