



BÁO CÁO THỰC HÀNH

Bài thực hành số 02: THU THẬP THÔNG TIN

Môn học: An toàn mạng máy tính

Lớp: NT101.N12.ATCL.1

THÀNH VIÊN THỰC HIỆN (Nhóm 05):

STT	Họ và tên	MSSV
1	Vũ Hoàng Thạch Thiết	20521957
2	Nguyễn Hùng Thịnh	20521963
3	Dương Đỗ Khoa	20521465

ĐÁNH GIÁ KHÁC:

Tổng thời gian thực hiện	
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

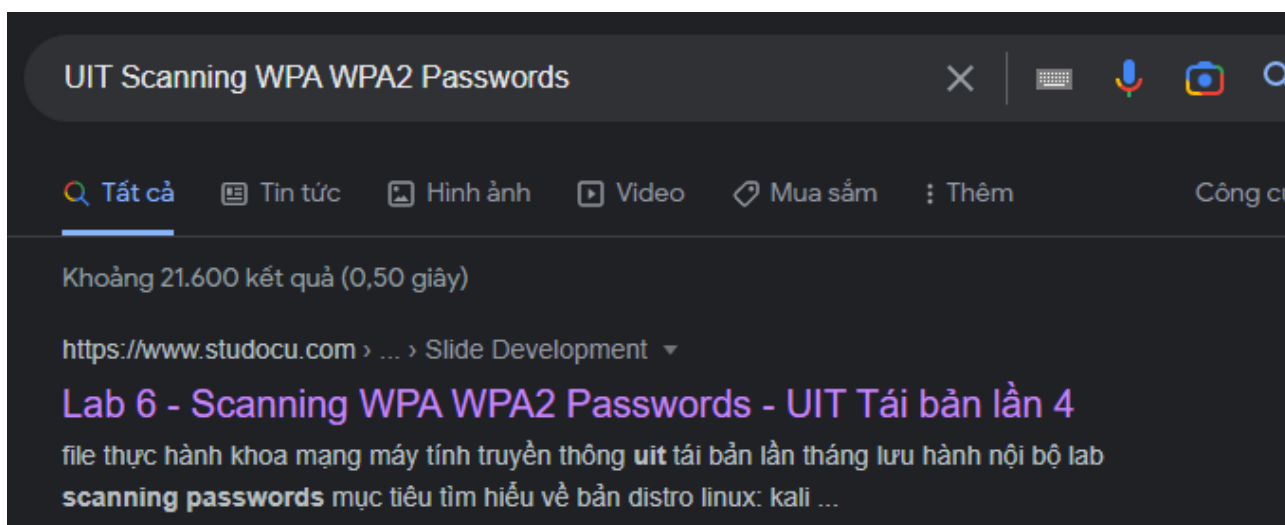
A. BÁO CÁO CHI TIẾT	3
1. Thu thập thông tin thụ động (Passive Information Gathering).....	3
Câu 10. Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?	3
Câu 14. Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG	3
2. Thu thập thông tin chủ động (Active Information Gathering).....	4
a. Liệt kê các bản ghi khác của DNS.....	4
b. Sử dụng lệnh host để tìm kiếm các bản ghi TXT, MX cho tên miền uit.edu.vn	4
Câu 21. Sử dụng lệnh host cho các hostname không tồn tại trong tên miền uit.edu.vn (idontexist, noexist, baithuchanhso2). Có nhận xét gì về kết quả trả về hay không? Giải thích?	5
Câu 22. Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com	6
Câu 23. Viết một chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM (hcmus.edu.vn, hcmussh.edu.vn, uit.edu.vn, hcmut.edu.vn, hcmiu.edu.vn, uel.edu.vn, hcmier.edu.vn, vnuhcm.edu.vn) và thực hiện zone transfer ứng với các nameserver đã tìm được.....	6
Câu 24. Viết Liệt kê danh sách các loại enumeration có thể được sử dụng cùng với tùy chọn -t.....	9
Câu 25. Cho một vài ví dụ sử dụng kết hợp các tùy chọn được DNSRecon hỗ trợ khác (ít nhất là 2 ví dụ)	9
Câu 26. So sánh 2 công cụ DNSEnum và DNSRecon? Công cụ nào dễ sử dụng hơn? Công cụ nào cho kết quả chính xác hơn? Công cụ nào hiển thị nhiều kết quả hơn?.....	11
Câu 27. Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan sử dụng Nmap.	13
Câu 28. Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan sử dụng Nmap.	13
Câu 29. So sánh với sử dụng phương thức SYN Scan (số lượng gói tin được gửi, số lượng gói tin được nhận, thời gian quét, kết quả hiển thị...)	14
Câu 30. Thực hiện kiểm tra các host đang hoạt động trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, ...)	14
Câu 31. Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn	15
Câu 32. Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP).....	16
Câu 33. Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)	19
B. TÀI LIỆU THAM KHẢO.....	21

A. BÁO CÁO CHI TIẾT

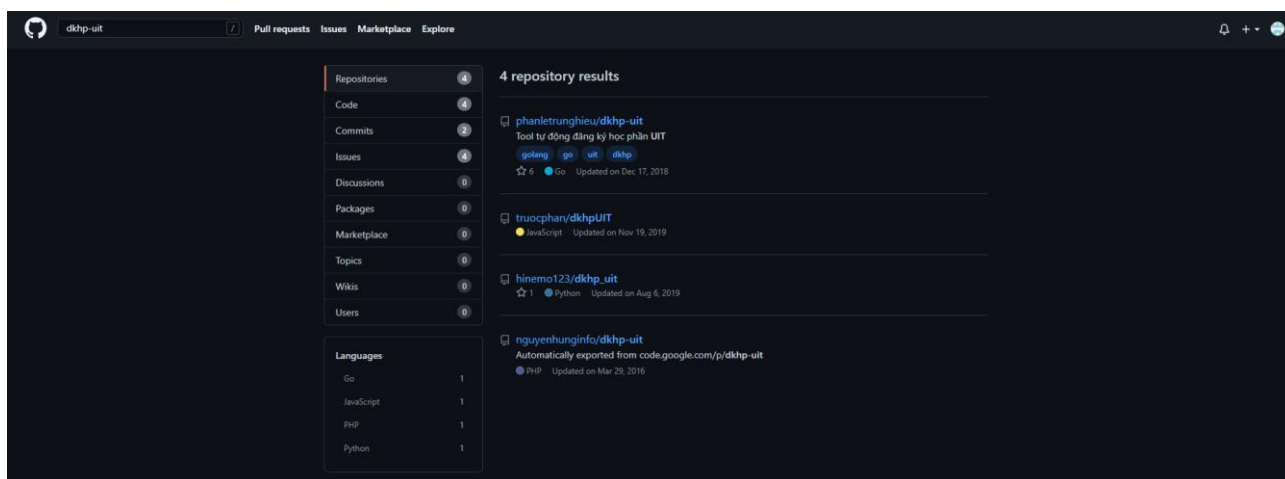
1. Thu thập thông tin thụ động (Passive Information Gathering)

Câu 10. Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?

Trong môn học Nhập môn Mạng máy tính, bài thực hành crack wifi là tài liệu lưu hành nội bộ của trường, tuy nhiên, chỉ với thao tác search đơn giản trên google, bất cứ ai cũng có thể tiếp cận bài lab đó:



Hoặc một số tool đăng kí học phần được đăng tải trên github, điều này làm ảnh hưởng đến quá trình đăng kí học phần cho nhiều sinh viên.



Câu 14. Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG

+) Sau khi cài đặt gitleaks:

```

$ gitleaks --help
Gitleaks scans code, past or present, for secrets

Usage:
  gitleaks [command]

Available Commands:
  completion  Generate the autocompletion script for the specified shell
  detect      detect secrets in code
  help        Help about any command
  protect     protect secrets in code
  version     display gitleaks version

Flags:
  -c, --config string      config file path
                           order of precedence:
                           1. --config/-c
                           2. env var GITLEAKS_CONFIG
                           3. (~source/-s)/.gitleaks.toml
                           If none of the three options are used, then gitleaks
                           will use the default config
  -e, --exit-code int      exit code when leaks have been encountered (default 1)
  -h, --help               help for gitleaks
  -l, --log-level string    log level (debug, info, warn, error, fatal) (default "info")
  -r, --redact              redact secrets from logs and stdout
  -f, --report-format string output format (json, csv, sarif) (default "json")
  -R, --report-path string  report file
  -s, --source string       path to source (default: $PWD) (default ".")
  -v, --verbose             show verbose output from scan
    
```

Tuy nhiên, em lại không tìm được repo của các trường đại học thành viên trong ĐHQG. Nên em chuyển qua cài Gitrob, và em không cài được...

2. Thu thập thông tin chủ động (Active Information Gathering)

a. Liệt kê các bản ghi khác của DNS

1. SOA (Start of Authority)

Trong mỗi tập tin cơ sở dữ liệu DNS có một và chỉ một record SOA. Bao gồm các thông tin về domain trên DNS Server, thông tin về zone transfer.

2. Record AAAA

Có nhiệm vụ tương tự A nhưng là địa chỉ Ipv6.

3. Record SRV

Bản ghi SRV được sử dụng để xác định vị trí các dịch vụ đặc biệt trong 1 domain, ví dụ tên máy chủ và số cổng của các máy chủ cho các dịch vụ được chỉ định.

4. Record DKIM

Là bản ghi dùng để xác thực người gửi bằng cách mã hóa một phần email gửi bằng một chuỗi ký tự, xem như là chữ ký.

5. Record SPF

Record SPF được tạo ra nhằm đảm bảo các máy chủ mail sẽ chấp nhận mail từ tên miền của khách hàng chỉ được gửi đi từ server của khách hàng. Sẽ giúp chống spam và giả mạo email.

b. Sử dụng lệnh host để tìm kiếm các bản ghi TXT, MX cho tên miền uit.edu.vn

+) Lệnh host để tìm kiếm các bản ghi TXT:

```
(kali㉿kali)-[~]
$ host -t txt uit.edu.vn
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C91tPny8NLttGS0aU5pJjKiY"
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"
```

+) Lệnh host để tìm kiếm các bản ghi MX:

```
(kali㉿kali)-[~]
$ host -t mx uit.edu.vn
uit.edu.vn mail is handled by 10 aspmx.l.google.com.
uit.edu.vn mail is handled by 20 alt2.aspmx.l.google.com.
uit.edu.vn mail is handled by 40 aspmx2.googlemail.com.
uit.edu.vn mail is handled by 40 aspmx3.googlemail.com.
uit.edu.vn mail is handled by 20 alt1.aspmx.l.google.com.
```

Câu 21. Sử dụng lệnh host cho các hostname không tồn tại trong tên miền uit.edu.vn (idontexist, noexist, baithuchanhso2). Có nhận xét gì về kết quả trả về hay không? Giải thích?

```
(kali㉿kali)-[~]
$ host dontexist.uit.edu.vn
dontexist.uit.edu.vn has address 45.122.249.78
dontexist.uit.edu.vn has address 118.69.123.142
```

```
(kali㉿kali)-[~]
$ host noexist.uit.edu.vn
noexist.uit.edu.vn has address 45.122.249.78
noexist.uit.edu.vn has address 118.69.123.142
```

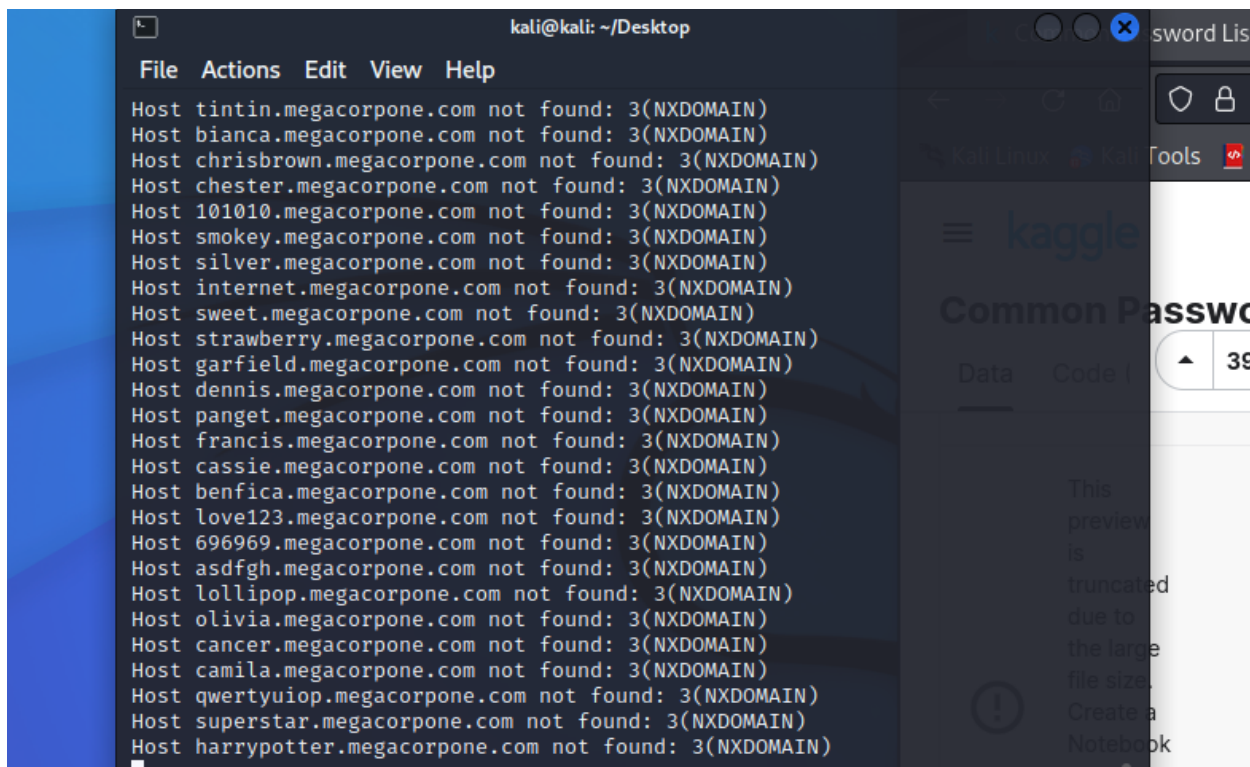
```
(kali㉿kali)-[~]
$ host baithuchanhso2.uit.edu.vn
baithuchanhso2.uit.edu.vn has address 118.69.123.142
baithuchanhso2.uit.edu.vn has address 45.122.249.78
```

```
(kali㉿kali)-[~]
$ host uit.edu.vn
uit.edu.vn has address 45.122.249.78
```

+) Có thể thấy rằng lệnh host cho các tên miền vẫn cho ra kết quả. Chứng tỏ DNS vẫn tồn tại các hostname này.

+) Thử tìm kiếm 2 địa chỉ IP trên thanh url của trình duyệt đều dẫn tới hostname uit.edu.vn.

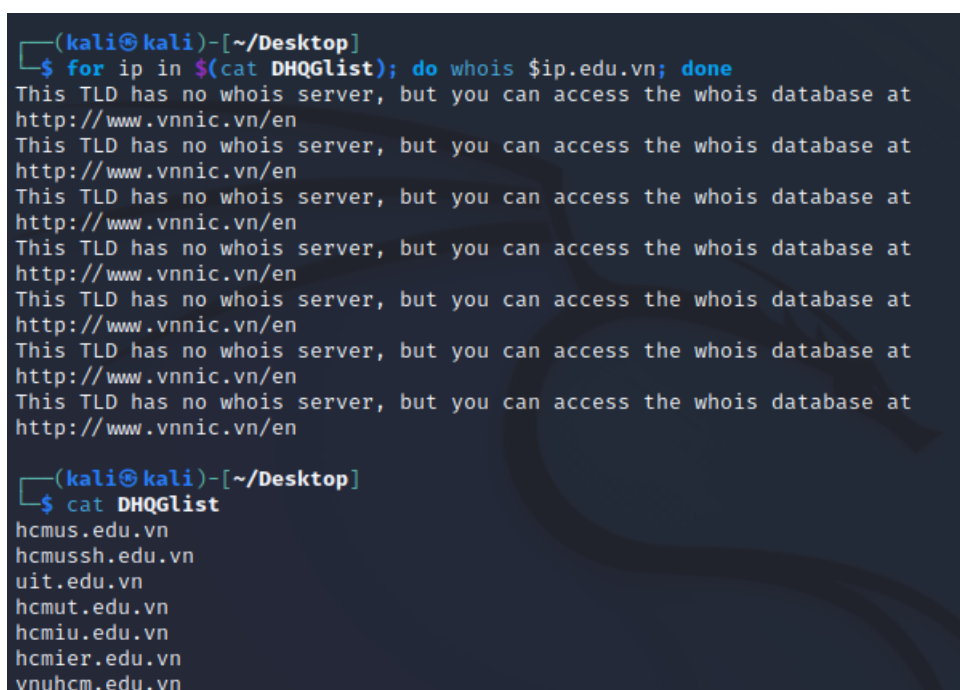
Câu 22. Sử dụng wordlist thông dụng khác (rockyou, seclists) để tìm kiếm các hostname hợp lệ khác của megacorpone.com



```
kali@kali: ~/Desktop
File Actions Edit View Help
Host tintin.megacorpone.com not found: 3(NXDOMAIN)
Host bianca.megacorpone.com not found: 3(NXDOMAIN)
Host chrisbrown.megacorpone.com not found: 3(NXDOMAIN)
Host chester.megacorpone.com not found: 3(NXDOMAIN)
Host 101010.megacorpone.com not found: 3(NXDOMAIN)
Host smokey.megacorpone.com not found: 3(NXDOMAIN)
Host silver.megacorpone.com not found: 3(NXDOMAIN)
Host internet.megacorpone.com not found: 3(NXDOMAIN)
Host sweet.megacorpone.com not found: 3(NXDOMAIN)
Host strawberry.megacorpone.com not found: 3(NXDOMAIN)
Host garfield.megacorpone.com not found: 3(NXDOMAIN)
Host dennis.megacorpone.com not found: 3(NXDOMAIN)
Host panget.megacorpone.com not found: 3(NXDOMAIN)
Host francis.megacorpone.com not found: 3(NXDOMAIN)
Host cassie.megacorpone.com not found: 3(NXDOMAIN)
Host benfica.megacorpone.com not found: 3(NXDOMAIN)
Host love123.megacorpone.com not found: 3(NXDOMAIN)
Host 696969.megacorpone.com not found: 3(NXDOMAIN)
Host asdfgh.megacorpone.com not found: 3(NXDOMAIN)
Host lollipop.megacorpone.com not found: 3(NXDOMAIN)
Host olivia.megacorpone.com not found: 3(NXDOMAIN)
Host cancer.megacorpone.com not found: 3(NXDOMAIN)
Host camila.megacorpone.com not found: 3(NXDOMAIN)
Host qwertyuiop.megacorpone.com not found: 3(NXDOMAIN)
Host superstar.megacorpone.com not found: 3(NXDOMAIN)
Host harrypotter.megacorpone.com not found: 3(NXDOMAIN)
```

Do danh sách quá dài nên em chỉ chụp 1 đoạn.

Câu 23. Viết một chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM (hcmus.edu.vn, hcmussh.edu.vn, uit.edu.vn, hcmut.edu.vn, hcmiu.edu.vn, uel.edu.vn, hcmier.edu.vn, vnuhcm.edu.vn) và thực hiện zone transfer ứng với các nameserver đã tìm được.



```
(kali@kali)-[~/Desktop]
$ for ip in $(cat DHQGLIST); do whois $ip.edu.vn; done
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en

(kali@kali)-[~/Desktop]
$ cat DHQGLIST
hcmus.edu.vn
hcmussh.edu.vn
uit.edu.vn
hcmut.edu.vn
hcmiu.edu.vn
hcmier.edu.vn
vnuhcm.edu.vn
```

Do không thể tìm ở đây nên em đã tìm ở trang web vnnic.vn và đây là danh sách:

Nameserver của UIT:

Máy chủ DNS chuyển giao: ns1.pavietnam.vn
ns2.pavietnam.vn
nsbak.pavietnam.net

Zone transfer

```
(kali㉿kali)-[~/Desktop]
$ host -l uit.edu.vn ns1.pavietnam.vn
Using domain server:
Name: ns1.pavietnam.vn
Address: 112.213.89.3#53
Aliases:

Host uit.edu.vn not found: 5(REFUSED)
; Transfer failed.

(kali㉿kali)-[~/Desktop]
$ host -l uit.edu.vn ns2.pavietnam.vn
Using domain server:
Name: ns2.pavietnam.vn
Address: 222.255.121.247#53
Aliases:

Host uit.edu.vn not found: 5(REFUSED)
; Transfer failed.

(kali㉿kali)-[~/Desktop]
$ host -l uit.edu.vn nsbak.pavietnam.vn
Using domain server:
Name: nsbak.pavietnam.vn
Address: 112.213.89.3#53
Aliases:
```

Nameserver của USSH, HCMIER và VNUHCM

Máy chủ DNS chuyển giao: server.vnuhcm.edu.vn
vnuserv.vnuhcm.edu.vn

Zone transfer

```
(kali㉿kali)-[~/Desktop]
$ host -l hcmussh.edu.vn server.vnuhcm.edu.vn
Using domain server:
Name: server.vnuhcm.edu.vn
Address: 103.88.121.201#53
Aliases:

Host hcmussh.edu.vn not found: 5(REFUSED)
; Transfer failed.

(kali㉿kali)-[~/Desktop]
$ host -l hcmussh.edu.vn vnuserv.vnuhcm.edu.vn
Using domain server:
Name: vnuserv.vnuhcm.edu.vn
Address: 103.88.121.200#53
Aliases:

Host hcmussh.edu.vn not found: 5(REFUSED)
; Transfer failed.
```

Tương tự với HCMIER và VNUHCM đều transfer failed.

Nameserver của HCMUS

Máy chủ DNS chuyển giao: dns1.hcmus.edu.vn
dns2.hcmus.edu.vn
server.hcmus.edu.vn

Zone transfer

```
(kali㉿kali)-[~/Desktop]
$ host -l hcmus.edu.vn dns1.hcmus.edu.vn
;; Connection to 14.241.254.131#53(14.241.254.131) for hcmus.edu.vn failed: t
imed out.
;; Connection to 14.241.254.131#53(14.241.254.131) for hcmus.edu.vn failed: t
imed out.

(kali㉿kali)-[~/Desktop]
$ host -l hcmus.edu.vn dns2.hcmus.edu.vn
;; Connection to 115.73.217.121#53(115.73.217.121) for hcmus.edu.vn failed: t
imed out.
;; Connection to 115.73.217.121#53(115.73.217.121) for hcmus.edu.vn failed: t
imed out.

(kali㉿kali)-[~/Desktop]
$ host -l hcmus.edu.vn server.hcmus.edu.vn
Using domain server:
Name: server.hcmus.edu.vn
Address: 171.244.202.180#53
Aliases:

Host hcmus.edu.vn not found: 5(REFUSED)
; Transfer failed.
```

Nameserver của HCMUT

Máy chủ DNS chuyển giao:	dns1.hcmut.edu.vn dns2.hcmut.edu.vn dns3.hcmut.edu.vn dns4.hcmut.edu.vn
--------------------------	--

Zone transfer

```
Aliases:

Host hcmut.edu.vn not found: 5(REFUSED)
; Transfer failed.

(kali㉿kali)-[~/Desktop]
$ host -l hcmut.edu.vn dns3.hcmut.edu.vn
Using domain server:
Name: dns3.hcmut.edu.vn
Address: 203.205.32.235#53
Aliases:

Host hcmut.edu.vn not found: 5(REFUSED)
; Transfer failed.

(kali㉿kali)-[~/Desktop]
$ host -l hcmut.edu.vn dns4.hcmut.edu.vn
Using domain server:
Name: dns4.hcmut.edu.vn
Address: 203.205.32.236#53
Aliases:

Host hcmut.edu.vn not found: 5(REFUSED)
; Transfer failed.
```

Tương tự với hostname dns1 và dns2.

Nameserver của HCMIU

Máy chủ DNS chuyển giao:	hcm-server1.vnn.vn vdc-hn01.vnn.vn
--------------------------	---------------------------------------


```
(kali㉿kali)-[~/Desktop]
$ host -l hcmiu.edu.vn hcm-server1.vnn.vn
Using domain server:
Name: hcm-server1.vnn.vn
Address: 203.162.4.1#53
Aliases:

Host hcmiu.edu.vn not found: 5(REFUSED)
; Transfer failed.

(kali㉿kali)-[~/Desktop]
$ host -l hcmiu.edu.vn vdc-hn01.vnn.vn
Using domain server:
Name: vdc-hn01.vnn.vn
Address: 203.162.0.11#53
Aliases:

Host hcmiu.edu.vn not found: 5(REFUSED)
; Transfer failed.
```

Nameserver của UEL

Máy chủ DNS chuyển giao:	ns1.dns.net.vn ns2.dns.net.vn
--------------------------	----------------------------------

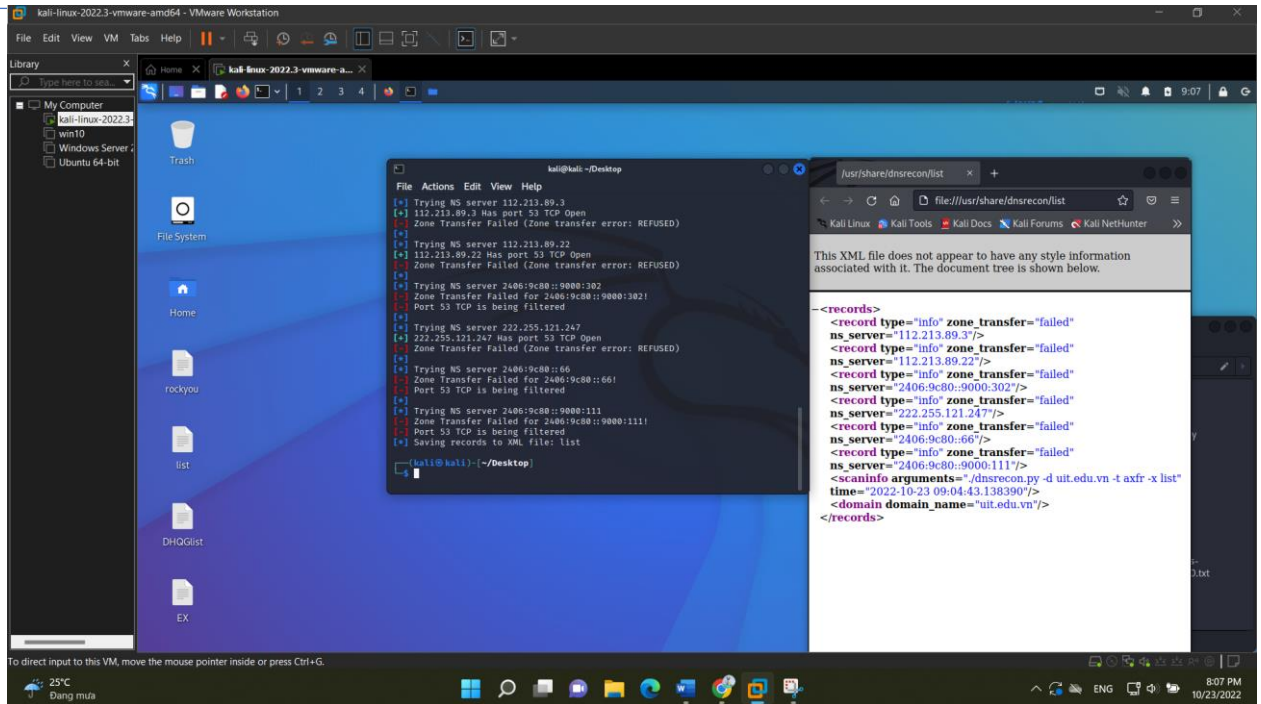
Tương tự với các trường hợp trên đều cho ra kết quả fail.

Câu 24. Viết Liệt kê danh sách các loại enumeration có thể được sử dụng cùng với tùy chọn -t

- t axfr: Zone transfer.
- t brt: brute force.
- t snoop: truy tìm bộ nhớ cache của DNS(Cache Snooping)
- t zonewalk: truy tìm các bản ghi nội bộ nếu zone không được cấu hình đúng cách.

Câu 25. Cho một vài ví dụ sử dụng kết hợp các tùy chọn được DNSRecon hỗ trợ khác (ít nhất là 2 ví dụ)

- x: lưu đầu ra vào 1 file.



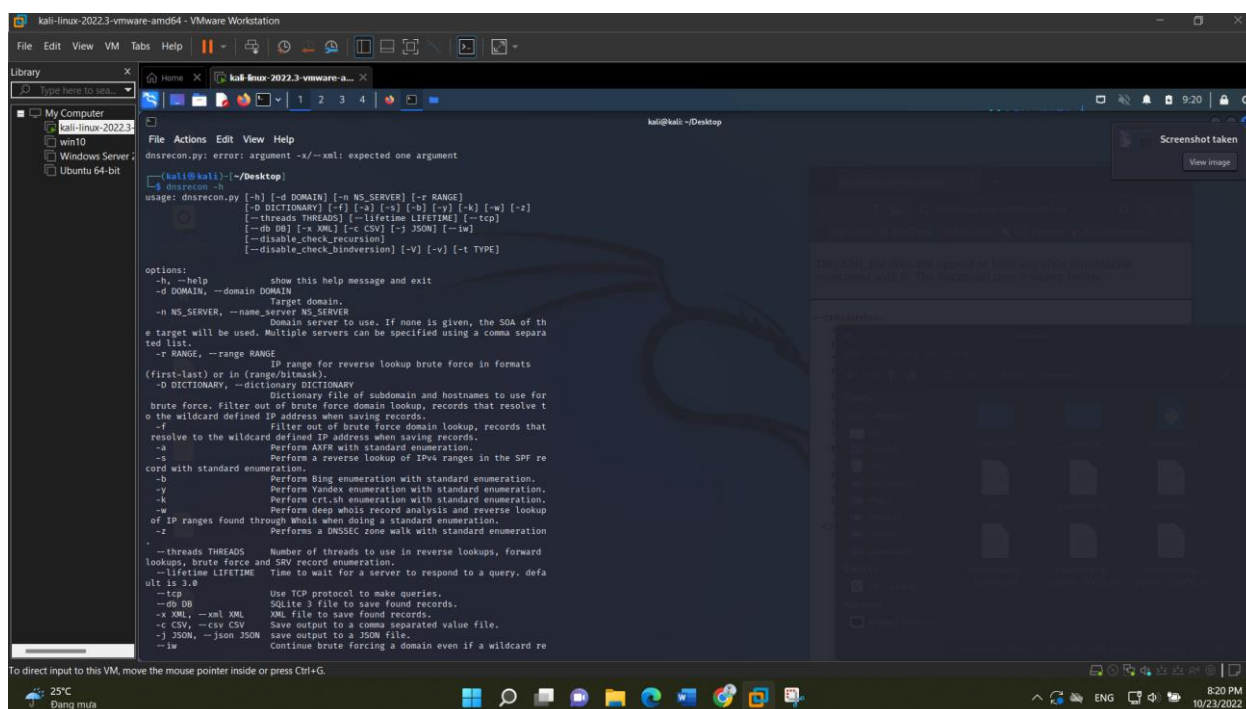
-a: Thực hiện AXFR với kiểu liệt kê tiêu chuẩn.

```
(kali@kali)-[~/Desktop]
$ sudo dnsrecon -d uit.edu.vn -t axfr -a
[*] Checking for Zone Transfer for uit.edu.vn name servers
[*] Resolving SOA Record
[+] SOA ns1.pavietnam.vn 112.213.89.3
[+] SOA ns1.pavietnam.vn 2406:9c80::66
[*] Resolving NS Records
[*] NS Servers found:
[+] NS nsbak.pavietnam.net 112.213.89.22
[+] NS nsbak.pavietnam.net 2406:9c80::9000:302
[+] NS ns1.pavietnam.vn 112.213.89.3
[+] NS ns1.pavietnam.vn 2406:9c80::66
[+] NS ns2.pavietnam.vn 222.255.121.247
[+] NS ns2.pavietnam.vn 2406:9c80::9000:111
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 2406:9c80::9000:111
[-] Zone Transfer Failed for 2406:9c80::9000:111!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 222.255.121.247
[+] 222.255.121.247 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 112.213.89.3
[+] 112.213.89.3 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 112.213.89.22
[+] 112.213.89.22 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 2406:9c80::9000:302
[-] Zone Transfer Failed for 2406:9c80::9000:302!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2406:9c80::66
[-] Zone Transfer Failed for 2406:9c80::66!
[-] Port 53 TCP is being filtered
```

--lifetime: Thời gian chờ máy chủ phản hồi một truy vấn. mặc định là 3.0

```
(kali@kali)-[~/Desktop]
$ sudo dnsrecon -d uit.edu.vn -t axfr --lifetime 5
[*] Checking for Zone Transfer for uit.edu.vn name servers
[*] Resolving SOA Record
[+] SOA ns1.pavietnam.vn 112.213.89.3
[+] SOA ns1.pavietnam.vn 2406:9c80::66
[*] Resolving NS Records
[*] NS Servers found:
[+] NS ns2.pavietnam.vn 222.255.121.247
[+] NS ns2.pavietnam.vn 2406:9c80::9000:111
[+] NS nsbak.pavietnam.net 112.213.89.22
[+] NS nsbak.pavietnam.net 2406:9c80::9000:302
[+] NS ns1.pavietnam.vn 112.213.89.3
[+] NS ns1.pavietnam.vn 2406:9c80::66
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 222.255.121.247
[+] 222.255.121.247 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 2406:9c80::9000:111
[-] Zone Transfer Failed for 2406:9c80::9000:111!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2406:9c80::66
```

Dưới đây là các tùy chọn của dnsrecon



Câu 26. So sánh 2 công cụ DNSEnum và DNSRecon? Công cụ nào dễ sử dụng hơn? Công cụ nào cho kết quả chính xác hơn? Công cụ nào hiển thị nhiều kết quả hơn?

Công cụ DNSEnum dễ sử dụng hơn do cú pháp đơn giản hơn.

```
(kali@kali)-[~]
$ dnsenum megacorpone.com
dnsenum VERSION:1.2.6

(kali@kali)-[~]
$ dnsrecon -d megacorpone.com -t axfr
```

Cả 2 đều cho ra kết quả chính xác như nhau.

```
Trying NS server 51.222.39.63
51.222.39.63 Has port 53 TCP Open
Zone Transfer was successful!!
NS ns1.megacorpone.com 51.79.37.18
NS ns2.megacorpone.com 51.222.39.63
NS ns3.megacorpone.com 66.70.207.180
TXT Try Harder
TXT google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA
MX @.megacorpone.com fb.mail.gandi.net 217.70.178.217
MX @.megacorpone.com fb.mail.gandi.net 217.70.178.215
MX @.megacorpone.com fb.mail.gandi.net 217.70.178.216
MX @.megacorpone.com spool.mail.gandi.net 217.70.178.1
A admin.megacorpone.com 51.222.169.208
A beta.megacorpone.com 51.222.169.209
A fs1.megacorpone.com 51.222.169.210
A intranet.megacorpone.com 51.222.169.211
A mail.megacorpone.com 51.222.169.212
A mail2.megacorpone.com 51.222.169.213
A ns1.megacorpone.com 51.79.37.18
A ns2.megacorpone.com 51.222.39.63
A ns3.megacorpone.com 66.70.207.180
A router.megacorpone.com 51.222.169.214
A siem.megacorpone.com 51.222.169.215
A snmp.megacorpone.com 51.222.169.216
A support.megacorpone.com 51.222.169.218
A syslog.megacorpone.com 51.222.169.217
A test.megacorpone.com 51.222.169.219
A vpn.megacorpone.com 51.222.169.220
```

```
Trying Zone Transfer for megacorpone.com on ns1.megacorpone.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for megacorpone.com on ns3.megacorpone.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for megacorpone.com on ns2.megacorpone.com ...
megacorpone.com. 300 IN SOA (
megacorpone.com. 300 IN TXT "Try
megacorpone.com. 300 IN TXT (
megacorpone.com. 300 IN MX 10
megacorpone.com. 300 IN MX 20
megacorpone.com. 300 IN MX 50
megacorpone.com. 300 IN MX 60
megacorpone.com. 300 IN NS ns1.megacorpone.com.
megacorpone.com. 300 IN NS ns2.megacorpone.com.
megacorpone.com. 300 IN NS ns3.megacorpone.com.
admin.megacorpone.com. 300 IN A 51.222.169.208
beta.megacorpone.com. 300 IN A 51.222.169.209
fs1.megacorpone.com. 300 IN A 51.222.169.210
intranet.megacorpone.com. 300 IN A 51.222.169.211
mail.megacorpone.com. 300 IN A 51.222.169.212
mail2.megacorpone.com. 300 IN A 51.222.169.213
ns1.megacorpone.com. 300 IN A 51.79.37.18
ns2.megacorpone.com. 300 IN A 51.222.39.63
ns3.megacorpone.com. 300 IN A 66.70.207.180
router.megacorpone.com. 300 IN A 51.222.169.214
siem.megacorpone.com. 300 IN A 51.222.169.215
snmp.megacorpone.com. 300 IN A 51.222.169.216
support.megacorpone.com. 300 IN A 51.222.169.218
syslog.megacorpone.com. 300 IN A 51.222.169.217
test.megacorpone.com. 300 IN A 51.222.169.219
vpn.megacorpone.com. 300 IN A 51.222.169.220
www.megacorpone.com. 300 IN A 149.56.244.87
```

Với cú pháp thông thường không thêm các tùy chọn DNSenum sẽ cho ra kết quả nhiều hơn do nó thực hiện nhiều công việc hơn, tuy nhiên với DNSRecon vẫn có thể cho ra nhiều kết quả nhưng sẽ phải thực hiện nhiều dòng lệnh hơn.

Câu 27. Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện SYN Scan sử dụng Nmap.

```
(kali㉿kali)-[~]
$ sudo nmap -sS uit.edu.vn
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 21:30 +07
Nmap scan report for uit.edu.vn (45.122.249.78)
Host is up (0.039s latency).
rDNS record for 45.122.249.78: static.cmcti.vn
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 52.40 seconds

(kali㉿kali)-[~]
$
```

39.10	vmware_1:1:03:84	broadcast	ARP	42 who has 192.168.152.27 Tell 192.168.152.128
er:19	45.122.249.78	192.168.152.128	TCP	60 135 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
11:11	45.122.249.78	192.168.152.128	TCP	60 23 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
er:11	45.122.249.78	192.168.152.128	TCP	60 995 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
11	45.122.249.78	192.168.152.128	TCP	60 1723 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
m:11	45.122.249.78	192.168.152.128	TCP	60 1720 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
5.0	45.122.249.78	192.168.152.128	TCP	60 21 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
sc:11	45.122.249.78	192.168.152.128	TCP	60 22 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
ca:11	45.122.249.78	192.168.152.128	TCP	60 53 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
06:11	45.122.249.78	192.168.152.128	TCP	60 111 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
er:19	45.122.249.78	192.168.152.128	TCP	60 110 → 48278 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
06:19	45.122.249.78	192.168.152.128	TCP	60 1720 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
er:19	45.122.249.78	192.168.152.128	TCP	60 110 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
19	45.122.249.78	192.168.152.128	TCP	60 111 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
0	45.122.249.78	192.168.152.128	TCP	60 21 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
0	45.122.249.78	192.168.152.128	TCP	60 22 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
or:10	45.122.249.78	192.168.152.128	TCP	60 995 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
28:14	45.122.249.78	192.168.152.128	TCP	60 135 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
15:15	45.122.249.78	192.168.152.128	TCP	60 53 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
re:15	45.122.249.78	192.168.152.128	TCP	60 23 → 48280 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

+ Ta thấy trong wire shark thì ip đích gửi trả kết quả lại cho máy tính những gói bị RST để có thể đóng kết nối trong quá trình bắt tay 3 bước nhưng không được

18	192.168.152.128	45.122.249.78	TCP	58 48278 → 1035 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	45.122.249.78	192.168.152.128	TCP	60 80 → 48278 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
17	192.168.152.128	45.122.249.78	TCP	54 48278 → 80 [RST] Seq=1 Win=0 Len=0
11	192.168.152.128	45.122.249.78	TCP	58 48278 → 32772 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	45.122.249.78	192.168.152.128	TCP	60 443 → 48278 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16	192.168.152.128	45.122.249.78	TCP	54 48278 → 443 [RST] Seq=1 Win=0 Len=0
14	192.168.152.128	45.122.249.78	TCP	58 48278 → 16080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

+ Máy ta bắt được 2 gói tin gửi từ máy cá nhân đến uit.edu.vn có port được mở là 80 và 443

Câu 28. Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan sử dụng Nmap.

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -sT uit.edu.vn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 21:42 +07
Nmap scan report for uit.edu.vn (45.122.249.78)
Host is up (0.0055s latency).
rDNS record for 45.122.249.78: static.cmcti.vn
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 61.75 seconds
```

3141	63.887655720	VMware_71:03:84	VMware_f9:62:5e	ARP	42 Who has 192.168.152.2? Tell 192.168.152.12
3142	63.891498812	192.168.152.128	45.122.249.78	TCP	74 52968 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
3143	63.992270348	192.168.152.128	45.122.249.78	TCP	74 54630 → 7800 [SYN] Seq=0 Win=64240 Len=0 N
3144	64.066113467	45.122.249.78	192.168.152.128	TCP	60 80 → 43088 [SYN, ACK] Seq=0 Ack=1 Win=6424

+) Ta thấy có gửi lại gói ACK để đóng kết nối

Câu 29. So sánh với sử dụng phương thức SYN Scan (số lượng gói tin được gửi, số lượng gói tin được nhận, thời gian quét, kết quả hiển thị...)

- + Với SYN Scan thì thời gian quét nhanh hơn vì số lượng gói tin được gửi đi ít hơn do không có gói ACK để hoàn tất quá trình bắt tay 3 bước
- + Còn với TCP Connect Scan thì ngược lại. Thời gian quét lâu hơn và số lượng gói cũng nhiều hơn vì có gửi gói ACK để xác nhận hoàn tất quá trình bắt tay 3 bước
- + Thấy số lượng gói tin nhận thì TCP Connect scan cũng nhiều hơn do số gói gửi đi cũng nhiều hơn SYN Scan

Câu 30. Thực hiện kiểm tra các host đang hoạt trong mạng bằng các ngôn ngữ lập trình khác (Bash script, Python, C/C++, Perl, ...)

```
File Actions Edit View Help
#!/bin/bash
for i in `seq ${2} ${3}`
do
    ping -c 1 ${1}.${i} > /dev/null 2>&1
    if [ $? -eq 0 ]; then
        echo "${1}.${i} responded."
    else
        echo "${1}.${i} did not respond."
    fi
done
~
~
```

+ Source code

```
(kali@kali)-[~/Desktop]
$ bash host_check.sh 192.168.152 1 254
192.168.152.1 responded.
192.168.152.2 responded.
192.168.152.3 did not respond.
192.168.152.4 did not respond.
192.168.152.5 did not respond.
192.168.152.6 did not respond.
192.168.152.7 did not respond.
192.168.152.8 did not respond.
192.168.152.9 did not respond.
192.168.152.10 did not respond.
192.168.152.11 did not respond.
192.168.152.12 did not respond.
192.168.152.13 did not respond.
192.168.152.14 did not respond.
192.168.152.15 did not respond.
192.168.152.16 did not respond.
192.168.152.17 did not respond.
```

+ Kết quả ta quét được có host 192.152.1.1 và host 192.168.152.2 đang hoạt động


```
(kali㉿kali)-[~/Desktop]
$ grep Up ping-sweep.txt | cut -d " " -f 2
192.168.152.1
192.168.152.2
192.168.152.128
```

+ So sánh với nmap sweep thì cũng tương tự nhưng ở trên chưa quét xong

Câu 31. Sử dụng Wireshark để phân tích gói tin khi sử dụng Nmap với tùy chọn -sn

Time	Source	Destination	Protocol	Length	Info
160	9.031622292	192.168.152.128	ICMP	42	Echo (ping) request id=0x6b52, seq=0/0, ttl=41 (no response found!)
161	9.031661364	192.168.152.128	ICMP	42	Echo (ping) request id=0x094e, seq=0/0, ttl=53 (no response found!)
162	9.031708099	192.168.152.128	ICMP	42	Echo (ping) request id=0x0802, seq=0/0, ttl=44 (no response found!)
163	9.031735470	192.168.152.128	ICMP	42	Echo (ping) request id=0xe88a, seq=0/0, ttl=39 (no response found!)
164	9.031777296	192.168.152.128	ICMP	42	Echo (ping) request id=0xa0d6, seq=0/0, ttl=42 (no response found!)
165	9.031804416	192.168.152.128	ICMP	42	Echo (ping) request id=0x9feb, seq=0/0, ttl=38 (no response found!)
166	9.031844951	192.168.152.128	ICMP	42	Echo (ping) request id=0xe721, seq=0/0, ttl=37 (no response found!)
167	9.031872070	192.168.152.128	ICMP	42	Echo (ping) request id=0x3b42, seq=0/0, ttl=39 (no response found!)
168	9.031913416	192.168.152.128	ICMP	42	Echo (ping) request id=0xd8ff, seq=0/0, ttl=46 (no response found!)
169	9.031950805	192.168.152.128	ICMP	42	Echo (ping) request id=0x3f31, seq=0/0, ttl=47 (no response found!)
170	9.031992211	192.168.152.128	ICMP	42	Echo (ping) request id=0x08eb, seq=0/0, ttl=59 (no response found!)
171	9.032019972	192.168.152.128	ICMP	42	Echo (ping) request id=0x9cf7, seq=0/0, ttl=53 (no response found!)
172	9.032062891	192.168.152.128	ICMP	42	Echo (ping) request id=0xfc82, seq=0/0, ttl=49 (no response found!)
173	9.032138099	192.168.152.128	ICMP	42	Echo (ping) request id=0xf377, seq=0/0, ttl=52 (no response found!)
174	9.032251837	192.168.152.128	ICMP	42	Echo (ping) request id=0x06e2, seq=0/0, ttl=52 (no response found!)
175	9.032327406	192.168.152.128	ICMP	42	Echo (ping) request id=0x6146, seq=0/0, ttl=52 (no response found!)
176	9.032479555	192.168.152.128	ICMP	42	Echo (ping) request id=0x5015, seq=0/0, ttl=45 (no response found!)
177	9.032603902	192.168.152.128	ICMP	42	Echo (ping) request id=0x74aa, seq=0/0, ttl=45 (no response found!)
178	9.032672129	192.168.152.128	ICMP	42	Echo (ping) request id=0x051f, seq=0/0, ttl=51 (no response found!)
179	9.117369230	192.168.152.128	ICMP	42	Echo (ping) request id=0xfa3d, seq=0/0, ttl=50 (no response found!)
180	9.117453895	192.168.152.128	ICMP	42	Echo (ping) request id=0x5865, seq=0/0, ttl=39 (no response found!)
181	9.117460788	192.168.152.128	ICMP	42	Echo (ping) request id=0x1011, seq=0/0, ttl=52 (no response found!)
182	9.117485634	192.168.152.128	ICMP	42	Echo (ping) request id=0xaa11, seq=0/0, ttl=54 (no response found!)
183	9.117492256	192.168.152.128	ICMP	42	Echo (ping) request id=0x6801, seq=0/0, ttl=55 (no response found!)
184	9.127645523	192.168.152.128	ICMP	42	Echo (ping) request id=0x29fa, seq=0/0, ttl=45 (no response found!)
185	9.127659087	192.168.152.128	ICMP	42	Echo (ping) request id=0x3ccc, seq=0/0, ttl=59 (no response found!)
186	9.127708999	192.168.152.128	ICMP	42	Echo (ping) request id=0x75af, seq=0/0, ttl=54 (no response found!)
187	9.127716282	192.168.152.128	ICMP	42	Echo (ping) request id=0xd0de, seq=0/0, ttl=43 (no response found!)
188	9.127741108	192.168.152.128	ICMP	42	Echo (ping) request id=0x1709, seq=0/0, ttl=56 (no response found!)
189	9.127748431	192.168.152.128	ICMP	42	Echo (ping) request id=0xe57d, seq=0/0, ttl=54 (no response found!)
190	9.127780961	192.168.152.128	ICMP	42	Echo (ping) request id=0xa474, seq=0/0, ttl=43 (no response found!)
191	9.127787964	192.168.152.128	ICMP	42	Echo (ping) request id=0xa474, seq=0/0, ttl=47 (no response found!)
192	9.127834119	192.168.152.128	ICMP	42	Echo (ping) request id=0x8577, seq=0/0, ttl=45 (no response found!)

+ Ta thấy nó gửi 1 loạt gói tin ICMP request tới các host xem có host nào phản hồi

234	9.140610263	192.168.152.128	ICMP	42	Echo (ping) request id=0x0e29, seq=0/0, ttl=59 (no response found!)
255	9.140610263	45.122.249.213	ICMP	60	Echo (ping) reply id=0x35fb, seq=0/0, ttl=128 (request in 231)
256	9.140842835	45.122.249.222	ICMP	60	Echo (ping) reply id=0xf83f, seq=0/0, ttl=128 (request in 238)
257	9.140843125	45.122.249.220	ICMP	60	Echo (ping) reply id=0x0cf7, seq=0/0, ttl=128 (request in 236)

+ Có host 192.168.152.125 có gói reply ở vị trí 231, 238, 236

238	9.134720937	192.168.152.128	ICMP	42	Echo (ping) request id=0xf83f, seq=0/0, ttl=46 (reply in 256)
239	9.134720937	192.168.152.128	ICMP	42	Echo (ping) request id=0x035f, seq=0/0, ttl=54 (no response found!)

+ Gói ICMP reply

269	9.227933403	192.168.152.128	ICMP	42	Echo (ping) request id=0x1070, seq=0/0, ttl=57 (reply in 234)
270	9.227975701	192.168.152.128	TCP	58	43092 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
271	9.228022397	192.168.152.128	TCP	58	43092 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
272	9.230888216	192.168.152.128	TCP	58	43092 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
273	9.230990604	192.168.152.128	TCP	58	43092 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
274	9.231040476	192.168.152.128	TCP	58	43092 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
275	9.231128998	192.168.152.128	TCP	58	43092 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
276	9.231211309	192.168.152.128	TCP	58	43092 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
277	9.231205202	192.168.152.128	ICMP	42	Echo (ping) request id=0x5828, seq=0/0, ttl=53 (no response found!)

+ Ngoài ra nó còn gửi gói TCP Syn đến Port 443

370	9.328567255	192.168.152.128	TCP	54	43092 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
371	9.328599595	192.168.152.128	TCP	54	43092 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
372	9.328630461	192.168.152.128	TCP	54	43092 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0

+ Và gói tin TCP ACK đến port 80

462	9.340966783	192.168.152.128	TCP	54	43092 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
463	9.341001536	192.168.152.128	ICMP	54	Timestamp request id=0x1980, seq=0/0, ttl=41
464	9.341008159	192.168.152.128	ICMP	54	Timestamp request id=0x2d0f, seq=0/0, ttl=44
465	9.341040518	192.168.152.128	ICMP	54	Timestamp request id=0x6043, seq=0/0, ttl=43
466	9.341047010	192.168.152.128	ICMP	54	Timestamp request id=0x2917, seq=0/0, ttl=54
467	9.341080131	192.168.152.128	ICMP	54	Timestamp request id=0xe159, seq=0/0, ttl=45
468	9.341086522	192.168.152.128	ICMP	54	Timestamp request id=0x3d00, seq=0/0, ttl=52

+ Nó cũng gửi những gói ICMP timestamp request đến từng host để xác minh máy host có sẵn hay không

Câu 32. Liệt kê các banner, dịch vụ đang chạy trên máy Metasploitable 2 (chỉ liệt kê các dịch vụ TCP)

```
(root@kali)-[/home/kali]
# sudo nmap -sV -sT -A www.megacorpone.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-26 05:16 EDT
Nmap scan report for www.megacorpone.com (149.56.244.87)
Host is up (0.31s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:bd:1d:f0:c2:fb:c3:d8:48:ef:7f:5f:ba:34:1f:06 (RSA)
|   256 05:4e:c7:97:80:2e:68:73:64:9a:6f:4d:a3:6b:dd:1f (ECDSA)
|_  256 d3:ac:5a:e7:e4:55:49:29:4c:58:9f:23:ee:5e:14:bd (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-title: MegaCorp One - Nanotechnology Is the Future
|_ http-server-header: Apache/2.4.38 (Debian)
443/tcp   open  ssl/http Apache httpd 2.4.38
|_ http-title: MegaCorp One - Nanotechnology Is the Future
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_  http/1.1
|_ http-server-header: Apache/2.4.38 (Debian)
|_ ssl-cert: Subject: commonName=www.megacorpone.com
| Subject Alternative Name: DNS:www.megacorpone.com
| Not valid before: 2022-08-29T06:35:38
|_ Not valid after: 2022-11-27T06:35:37
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), Linux 3.2 (96%), Linux 4.4 (94%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (92%), Microsoft Windows XP SP3 (92%), BlueArc Titan 2100 NAS device (91%), VMware Player virtual NAT device (91%), Pirelli DP-10 VoIP phone (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   0.63 ms  192.168.17.2
2   ... 18
19  286.10 ms www.megacorpone.com (149.56.244.87)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.77 seconds
```

```
(kali㉿kali)-[~]
$ nmap -sV -sT -A 192.168.17.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-26 06:12 EDT
Nmap scan report for 192.168.17.133
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.17.129
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA
/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_ Not valid after:  2010-04-16T14:07:45
|_ ssl-date: 2022-10-26T10:10:28+00:00; -2m36s from scanner time.
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETR
N, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-title: Metasploitable2 - Linux
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```



```

|_ bind.version: 9.4.2
80/tcp open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-title: Metasploitable2 - Linux
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open  rpcbind    2 (RPC #100000)
|_ rpcinfo:
|   program version      port/proto  service
|   100000   2                111/tcp    rpcbind
|   100000   2                111/udp    rpcbind
|   100003   2,3,4           2049/tcp   nfs
|   100003   2,3,4           2049/udp   nfs
|   100005   1,2,3           45942/udp  mountd
|   100005   1,2,3           59095/tcp  mountd
|   100021   1,3,4           37856/udp  nlockmgr
|   100021   1,3,4           43842/tcp  nlockmgr
|   100024   1                34083/udp  status
|_  100024   1                52419/tcp  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login
514/tcp open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
|_ mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, SupportsCompression,
ConnectWithDatabase, Speaks41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandsha
ke
|   Status: Autocommit
|_  Salt: !u0jIj[i|W|.kS=wbeSP
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-date: 2022-10-26T10:10:28+00:00; -2m36s from scanner time.
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA
/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_ Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
|_ vnc-info:
|   Protocol version: 3.3
|   Security types:
|_   VNC Authentication (2)
6000/tcp open  X11         (access denied)

```

```

6667/tcp open  irc          UnrealIRCd
|_irc-info:
|_  users: 1
|_  servers: 1
|_  slusers: 1
|_  lservers: 0
|_  server: irc.Metasploitable.LAN
|_  version: Unreal3.2.8.1. irc.Metasploitable.LAN
|_  uptime: 0 days, 0:04:23
|_  source ident: nmap
|_  source host: C5918DCC.69B33A9E.FFFA6D49.IP
|_  error: Closing Link: qkpfhslmm[192.168.17.129] (Quit: qkpfhslmm)
8009/tcp open  ajp13          Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 57m23s, deviation: 2h00m00s, median: -2m36s
|_smb-security-mode:
|_  account_used: <blank>
|_  authentication_level: user
|_  challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb-os-discovery:
|_  OS: Unix (Samba 3.0.20-Debian)
|_  Computer name: metasploitable
|_  NetBIOS computer name:
|_  Domain name: localdomain
|_  FQDN: metasploitable.localdomain
|_  System time: 2022-10-26T06:10:20-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.80 seconds
    
```

Câu 33. Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)

*script=qscan

```

└─$ sudo nmap 192.168.17.133 --script=qscan
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-26 06:18 EDT
Nmap scan report for 192.168.17.133
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:17:50:1F (VMware)

Host script results:
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 1      0       606.70     136.39   0.0%
| 21     0       552.70     51.48    0.0%
| 22     0       767.30     497.13   0.0%
| 23     0       524.00     77.00    0.0%
| 25     0       547.50     117.02   0.0%
| 53     1       515.20     71.56    0.0%
| 80     0       547.20     80.96    0.0%
| 111    0       606.60     137.90   0.0%
| _139   0       597.80     164.89   0.0%

Nmap done: 1 IP address (1 host up) scanned in 20.14 seconds

```

*script=ssl-cert:


```
(kali㉿kali)-[~]
$ sudo nmap 192.168.17.133 --script=ssl-cert
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-26 06:20 EDT
Nmap scan report for 192.168.17.133
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA
| /stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPro
| vinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| MD5: dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA
| /stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPro
| vinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| MD5: dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:17:50:1F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 71.56 seconds
```

B. TÀI LIỆU THAM KHẢO