

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



BÁO CÁO THỰC HÀNH SỐ 1

Môn học: AN TOÀN MẠNG

Hệ thống tên miền và truy vấn thông tin tên miền

Tên sinh viên: Ninh Chí Hường

Mã sinh viên: B20DCAT094

Nhóm lớp : 01

Gi.ảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

HÀ NỘI, THÁNG 11/2023

Table of Contents

1. Mục đích :.....	2
2. Tìm hiểu về giao thức DNS và hệ thống tên miền.....	2
3. Nội dung thực hành	3
3.1 Cài đặt các công cụ, nền tảng.....	3
3.2 Tìm thông tin về tên miền sử dụng nslookup.....	3
3.3 Tìm thông tin về tên miền sử dụng các công cụ dig, dnsenum, dnsrecon và nmap	7

1. Mục đích :

- Tìm hiểu về giao thức DNS và hệ thống tên miền
- Luyện thực hành tìm thông tin về các tên miền sử dụng một số công cụ sẵn có

1.1 Các phần mềm, công cụ cần có

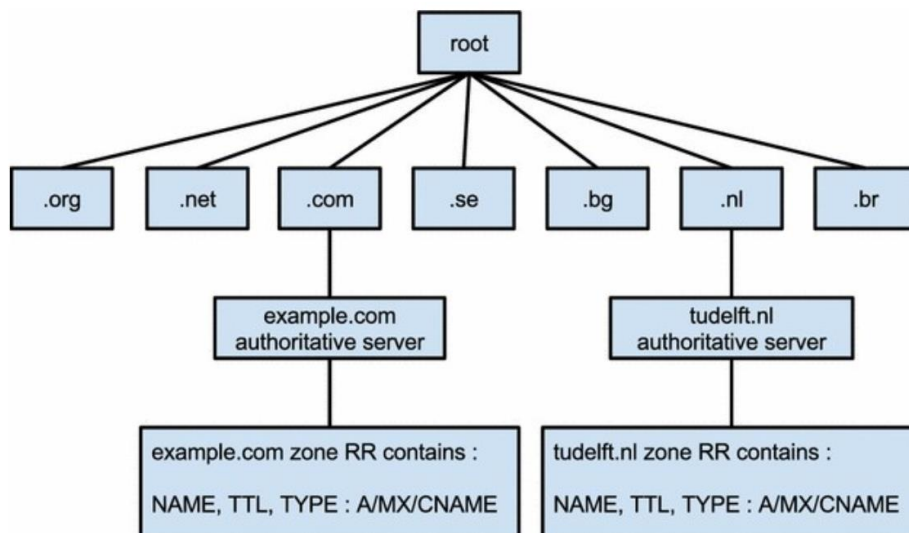
- Kali Linux và các công cụ trích xuất thông tin về các tên miền có sẵn trong Kali Linux:

- nslookup
- dig
- dnsenum
- dnsrecon
- nmap

2. Tìm hiểu về giao thức DNS và hệ thống tên miền

DNS (Domain Name System) là giao thức vận hành hệ thống tên miền. Hệ thống tên miền là một hệ thống giúp cho việc chuyển đổi các tên miền mà con người dễ ghi nhớ (dạng ký tự, ví dụ `www.example.com`) sang địa chỉ IP (dạng số, ví dụ `123.11.5.19`) tương ứng của tên miền đó. Cổng chuẩn của giao thức DNS là UDP 53. DNS giúp liên kết các tên với các thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị trên Internet.

DNS quản lý các tên miền theo mô hình cây (tree), gồm gốc (root) và các mức tên miền theo mô hình cây / phân cấp. Các máy chủ tên miền (DNS server) là thành phần quan trọng trong hệ thống tên miền: máy chủ lưu các thông tin về tên miền và cho phép chuyển đổi tên miền \leftrightarrow IP và ngược lại. Thông tin về các tên miền được lưu trong các file gọi là zone (vùng/miền).



3. Nội dung thực hành

3.1 Cài đặt các công cụ, nền tảng

- Cài đặt Kali Linux 2023 (nếu chưa cài đặt) trên 1 máy ảo (hoặc máy thực)
 - o Bản ISO của Kali Linux có thể tải tại: <https://www.kali.org/get-kali/#kali-baremetal>
 - o Bản cài sẵn trên máy ảo của Kali Linux có thể tải tại: <https://www.kali.org/getkali/#kali-virtual-machines>
- Kiểm tra xem trên Kali Linux đã có sẵn các công cụ nslookup, dig, dnsenum, dnsrecon và nmap chưa bằng cách gõ tên các công cụ này và chạy trong terminal

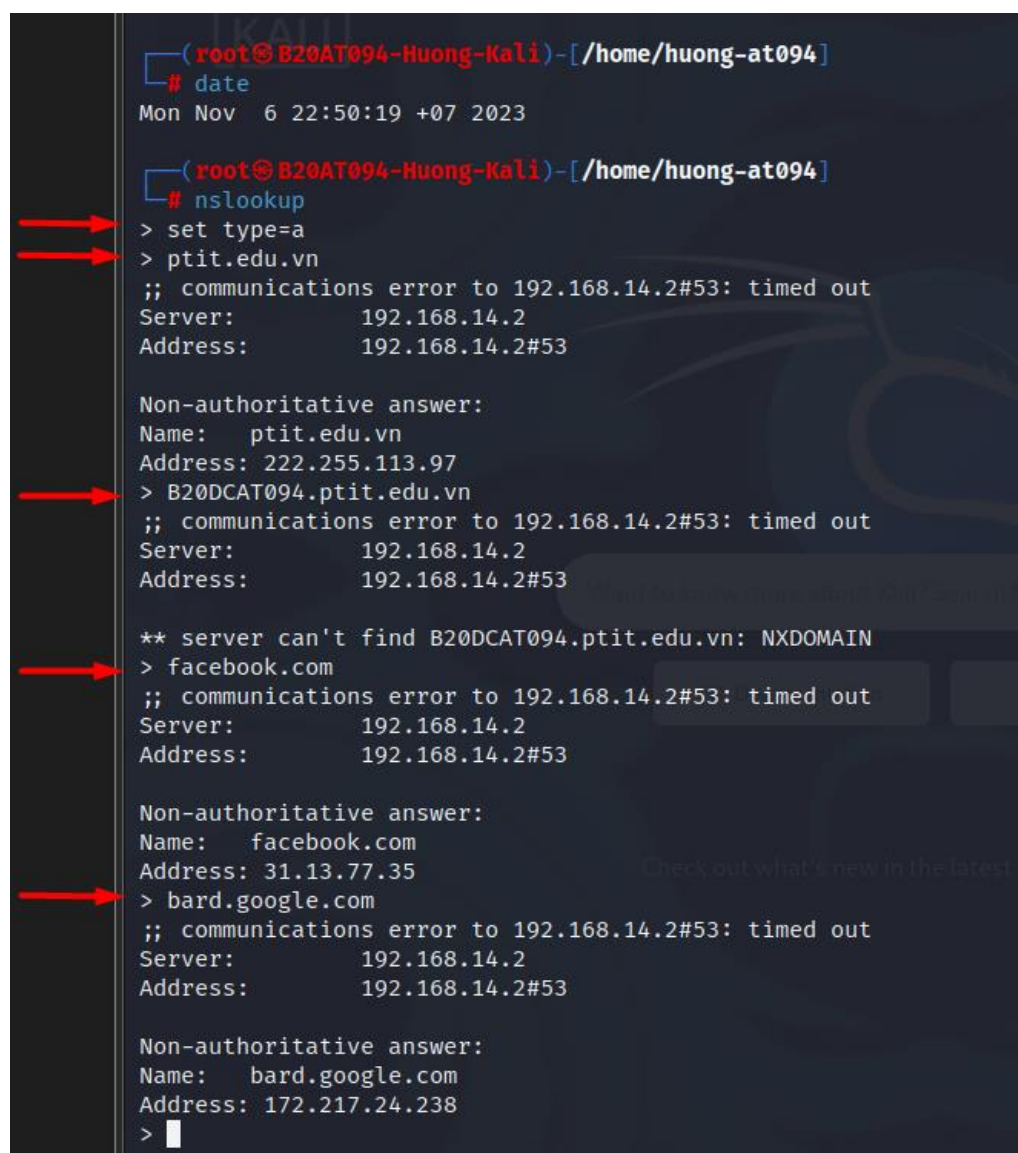
3.2 Tìm thông tin về tên miền sử dụng nslookup

- Khởi động *nslookup* trong cửa sổ terminal
- Tìm địa chỉ IP của các tên miền (thực hiện với 3 tên miền)

```
>set type = a
```

```
>ptit.edu.vn
```

```
>(ma_sv).ptit.edu.vn
```



```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Mon Nov 6 22:50:19 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# nslookup
> set type=a
> ptit.edu.vn
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
Name:   ptit.edu.vn
Address: 222.255.113.97
> B20DCAT094.ptit.edu.vn
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

** server can't find B20DCAT094.ptit.edu.vn: NXDOMAIN
> facebook.com
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
Name:   facebook.com
Address: 31.13.77.35
> bard.google.com
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
Name:   bard.google.com
Address: 172.217.24.238
>
```

- Tìm máy chủ DNS của các tên miền (thực hiện với 3 tên miền)

> set type = ns

> ptit.edu.vn

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Mon Nov 6 22:57:47 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# nslookup
> set type=ns
> ptit.edu.vn
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
ptit.edu.vn  nameserver = ns1.vdconline.vn.
ptit.edu.vn  nameserver = ns2.vdconline.vn.

Authoritative answers can be found from:
> google.com
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
google.com  nameserver = ns4.google.com.
google.com  nameserver = ns1.google.com.
google.com  nameserver = ns3.google.com.
google.com  nameserver = ns2.google.com.

Authoritative answers can be found from:
> facebook.com
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
facebook.com nameserver = c.ns.facebook.com.
facebook.com nameserver = b.ns.facebook.com.
facebook.com nameserver = d.ns.facebook.com.
facebook.com nameserver = a.ns.facebook.com.

Authoritative answers can be found from:
```

- Tìm máy chủ email của các tên miền (thực hiện với 3 tên miền)

>set type = mx

>ptit.edu.vn

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Mon Nov  6 23:04:17 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# nslookup
> set type=mx
> ptit.edu.vn
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
ptit.edu.vn  mail exchanger = 1 ptit-edu-vn.mail.eo.outlook.com.

Authoritative answers can be found from:
> google.com
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
google.com   mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
> microsoft.com
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
microsoft.com mail exchanger = 10 microsoft-com.mail.protection.outlook.com.

Authoritative answers can be found from:
> 
```


- Tìm tên miền tương ứng với địa chỉ IP (thực hiện với 3 địa chỉ IP)

>set type = ptr

>64.233.187.26

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Mon Nov 6 23:06:40 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# nslookup
> set type=ptr
> 64.233.187.26
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
26.187.233.64.in-addr.arpa      name = tj-in-f26.1e100.net.

Authoritative answers can be found from:
> 222.255.113.97
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
97.113.255.222.in-addr.arpa    name = static.vnpt.vn.

Authoritative answers can be found from:
> 31.13.77.35
;; communications error to 192.168.14.2#53: timed out
Server:      192.168.14.2
Address:     192.168.14.2#53

Non-authoritative answer:
35.77.13.31.in-addr.arpa      name = edge-star-mini-shv-01-hkt1.facebo
ok.com.

Authoritative answers can be found from:
> █
```

3.3 Tìm thông tin về tên miền sử dụng các công cụ dig, dnsenum, dnsrecon và nmap

- Sử dụng dig (thực hiện với 3 tên miền)

#dig ptit.edu.vn

1.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# dig ptit.edu.vn

; <<>> DiG 9.18.16-1-Debian <<>> ptit.edu.vn
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 8575
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;ptit.edu.vn.                IN      A
;; ANSWER SECTION:
ptit.edu.vn.                 5       IN      A      222.255.113.97

;; Query time: 24 msec
;; SERVER: 192.168.14.2#53(192.168.14.2) (UDP)
;; WHEN: Mon Nov 06 23:15:19 +07 2023
;; MSG SIZE rcvd: 56

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Mon Nov  6 23:15:24 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
#
```


2.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Mon Nov  6 23:15:24 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# dig google.com

; <<>> DiG 9.18.16-1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 33438
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 IN      A      172.217.27.46

;; Query time: 8 msec
;; SERVER: 192.168.14.2#53(192.168.14.2) (UDP)
;; WHEN: Mon Nov 06 23:16:44 +07 2023
;; MSG SIZE rcvd: 55
```

3.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Mon Nov  6 23:19:18 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# dig facebook.com

; <<>> DiG 9.18.16-1-Debian <<>> facebook.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 8429
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;facebook.com.              IN      A

;; ANSWER SECTION:
facebook.com.               IN      A      31.13.75.35

;; Query time: 8 msec
;; SERVER: 192.168.14.2#53(192.168.14.2) (UDP)
;; WHEN: Mon Nov 06 23:19:28 +07 2023
;; MSG SIZE rcvd: 57
```

- Sử dụng dnsenum (thực hiện với 3 tên miền)

#dnsenum --thread 15 -s ptit.edu.vn

1.

```
(root@B20AT094-Huong-Kali)~[/home/huong-at094]
# date
Fri Nov 10 13:44:55 +07 2023

(root@B20AT094-Huong-Kali)~[/home/huong-at094]
# dnsenum --thread 15 -s 5 ptit.edu.vn
dnsenum VERSION:1.2.6

----- ptit.edu.vn -----

Host's addresses:

ptit.edu.vn. 5 IN A 222.255.113.97

Wildcard detection using: pihpciktodgx

pihpciktodgx.ptit.edu.vn. 5 IN A 125.235.4.59

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Wildcards detected, all subdomains will point to the same IP address
Omitting results containing 125.235.4.59.
Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Name Servers:

ns1.vdconline.vn. 5 IN A 14.225.24.83
ns2.vdconline.vn. 5 IN A 14.225.24.84

Mail (MX) Servers:

ptit-edu-vn.mail.eo.outlook.com. 5 IN A 52.101.132.28
ptit-edu-vn.mail.eo.outlook.com. 5 IN A 52.101.132.30
ptit-edu-vn.mail.eo.outlook.com. 5 IN A 52.101.137.0
ptit-edu-vn.mail.eo.outlook.com. 5 IN A 52.101.137.2

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for ptit.edu.vn on ns1.vdconline.vn ...
AXFR record query failed: REFUSED

Trying Zone Transfer for ptit.edu.vn on ns2.vdconline.vn ...
AXFR record query failed: REFUSED

Scraping ptit.edu.vn subdomains from Google:

----- Google search page: 1 -----
----- Google search page: 2 -----
----- Google search page: 3 -----
hcm
----- Google search page: 4 -----
----- Google search page: 5 -----

Google Results:

hcm.ptit.edu.vn. 5 IN A 203.205.21.171

Brute forcing with /usr/share/dnsenum/dns.txt:

autodiscover.ptit.edu.vn. 5 IN CNAME autodiscover.outlook.com.
autodiscover.outlook.com. 5 IN CNAME atod-g2.tm-4.office.com.
atod-g2.tm-4.office.com. 5 IN A 40.99.10.56
atod-g2.tm-4.office.com. 5 IN A 40.99.10.8
atod-g2.tm-4.office.com. 5 IN A 40.99.10.72
atod-g2.tm-4.office.com. 5 IN A 40.99.10.24
```

atod-g2.tm-4.office.com.	5	IN	A	40.99.10.40
atod-g2.tm-4.office.com.	5	IN	A	40.99.10.120
atod-g2.tm-4.office.com.	5	IN	A	40.99.33.136
atod-g2.tm-4.office.com.	5	IN	A	52.98.54.136
it.ptit.edu.vn.	5	IN	A	222.255.113.97
jobs.ptit.edu.vn.	5	IN	A	203.162.88.104
mail.ptit.edu.vn.	5	IN	A	123.30.182.167
portal.ptit.edu.vn.	5	IN	A	222.255.113.97
www.ptit.edu.vn.	5	IN	A	222.255.113.97

ptit.edu.vn class C netranges:

123.30.182.0/24
203.162.88.0/24
203.205.21.0/24
222.255.113.0/24

Performing reverse lookup on 1024 ip addresses:

0 results out of 1024 IP addresses.

ptit.edu.vn ip blocks:

done.

2.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Fri Nov 10 13:46:06 +07 2023
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# dnsenum --thread 15 -s 5 viblo.asia
dnsenum VERSION:1.2.6
```

viblo.asia

Host's addresses:

viblo.asia.	5	IN	A	104.21.6.150
viblo.asia.	5	IN	A	172.67.134.232

Wildcard detection using: xvoghoveebjw

xvoghoveebjw.viblo.asia.	5	IN	A	125.235.4.59
--------------------------	---	----	---	--------------

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Wildcards detected, all subdomains will point to the same IP address
Omitting results containing 125.235.4.59.
Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Name Servers:

albert.ns.cloudflare.com.	5	IN	A	172.64.33.58
albert.ns.cloudflare.com.	5	IN	A	108.162.193.58
albert.ns.cloudflare.com.	5	IN	A	173.245.59.58
deb.ns.cloudflare.com.	5	IN	A	172.64.32.92
deb.ns.cloudflare.com.	5	IN	A	173.245.58.92
deb.ns.cloudflare.com.	5	IN	A	108.162.192.92

Mail (MX) Servers:

mx3.zoho.com.	5	IN	A	136.143.191.44
mx.zoho.com.	5	IN	A	136.143.191.44
mx2.zoho.com.	5	IN	A	136.143.191.44

File System

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for viblo.asia on albert.ns.cloudflare.com ...
AXFR record query failed: FORMERR

Trying Zone Transfer for viblo.asia on deb.ns.cloudflare.com ...
AXFR record query failed: FORMERR

Scraping viblo.asia subdomains from Google:

— Google search page: 1 —

— Google search page: 2 —

— Google search page: 3 —

— Google search page: 4 —

— Google search page: 5 —

Google Results:

perhaps Google is blocking our queries.
Check manually.

Brute forcing with /usr/share/dnsenum/dns.txt:

about.viblo.asia.	5	IN	A	104.21.6.150
about.viblo.asia.	5	IN	A	172.67.134.232
accounts.viblo.asia.	5	IN	A	104.21.6.150
accounts.viblo.asia.	5	IN	A	172.67.134.232
admin.viblo.asia.	5	IN	A	172.67.134.232
admin.viblo.asia.	5	IN	A	104.21.6.150
mail.viblo.asia.	5	IN	CNAME	u1402450.wl201.sendgrid.net.
www.viblo.asia.	5	IN	A	172.67.134.232
www.viblo.asia.	5	IN	A	104.21.6.150

viblo.asia class C netranges:

104.21.6.0/24
172.67.134.0/24

Performing reverse lookup on 512 ip addresses:

0 results out of 512 IP addresses.

viblo.asia ip blocks:

done.

3.

```
(root@820AT094-Huong-Kali)-[/home/huong-at094]
# date
Fri Nov 10 13:47:27 +07 2023

(root@820AT094-Huong-Kali)-[/home/huong-at094]
# dnsenum --thread 15 -s 5 dantri.com.vn
dnsenum VERSION:1.2.6

----- dantri.com.vn -----
Host's addresses:

dantri.com.vn.                5      IN      A       42.113.206.26

Wildcard detection using: bmbfohhnijqh

bmbfohhnijqh.dantri.com.vn.   5      IN      A       42.113.206.26

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Wildcards detected, all subdomains will point to the same IP address
Omitting results containing 42.113.206.26.
Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Name Servers:

ns2.dantri.com.vn.            5      IN      A       125.212.194.153
ns1.dantri.com.vn.            5      IN      A       42.113.206.23

Mail (MX) Servers:

aspmx.l.google.com.           5      IN      A       142.251.12.27
aspmx5.googlemail.com.        5      IN      A       64.233.171.27
alt1.aspmx.l.google.com.      5      IN      A       173.194.202.26
aspmx2.googlemail.com.        5      IN      A       173.194.202.26
aspmx4.googlemail.com.        5      IN      A       142.250.115.26
aspmx3.googlemail.com.        5      IN      A       142.250.141.27
alt2.aspmx.l.google.com.      5      IN      A       142.250.141.27

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for dantri.com.vn on ns2.dantri.com.vn ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for dantri.com.vn on ns1.dantri.com.vn ...
AXFR record query failed: NOTIMP

Scraping dantri.com.vn subdomains from Google:

-----
Google search page: 1
Google search page: 2
Google search page: 3
Google search page: 4
Google search page: 5

Google Results:

perhaps Google is blocking our queries.
Check manually.
```

Brute forcing with /usr/share/dnsenum/dns.txt:

ads.dantri.com.vn.	5	IN	A	42.113.206.9
beta.dantri.com.vn.	5	IN	A	42.113.206.59
form.dantri.com.vn.	5	IN	A	42.113.206.30
ftp.dantri.com.vn.	5	IN	A	42.113.206.12
live.dantri.com.vn.	5	IN	CNAME	47997f948d.newscdn.vn.
47997f948d.newscdn.vn.	5	IN	A	125.212.194.142
47997f948d.newscdn.vn.	5	IN	A	125.212.194.143
ns1.dantri.com.vn.	5	IN	A	42.113.206.23
ns2.dantri.com.vn.	5	IN	A	125.212.194.153
static.dantri.com.vn.	5	IN	A	42.113.206.30
test.dantri.com.vn.	5	IN	A	42.113.206.59

dantri.com.vn class C netranges:

42.113.206.0/24
125.212.194.0/24

Performing reverse lookup on 512 ip addresses:

0 results out of 512 IP addresses.

dantri.com.vn ip blocks:

done.

4.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Fri Nov 10 13:50:31 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# dnsenum --thread 15 -s 5 facebook.com
dnsenum VERSION:1.2.6

— facebook.com —

Host's addresses:

facebook.com.                5      IN      A       31.13.75.35

Wildcard detection using: yejvpbfiaqap

yejvpbfiaqap.facebook.com.   5      IN      A       125.235.4.59

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Wildcards detected, all subdomains will point to the same IP address
Omitting results containing 125.235.4.59.
Maybe you are using OpenDNS servers.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Name Servers:

a.ns.facebook.com.           5      IN      A       129.134.30.12
c.ns.facebook.com.           5      IN      A       185.89.218.12
b.ns.facebook.com.           5      IN      A       129.134.31.12
d.ns.facebook.com.           5      IN      A       185.89.219.12

Mail (MX) Servers:

smtpin.vvv.facebook.com.     5      IN      A       69.171.251.251

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for facebook.com on c.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on d.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on b.ns.facebook.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for facebook.com on a.ns.facebook.com ...
AXFR record query failed: timed out

Scraping facebook.com subdomains from Google:

— Google search page: 1 —

— Google search page: 2 —

— Google search page: 3 —

— Google search page: 4 —

— Google search page: 5 —

Google Results:

perhaps Google is blocking our queries.
Check manually.

Brute forcing with /usr/share/dnsenum/dns.txt:
```

Brute forcing with /usr/share/dnsenum/dns.txt:

about.facebook.com.	5	IN	CNAME	www.facebook.com.
www.facebook.com.	5	IN	CNAME	star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.	5	IN	A	31.13.75.35
ads.facebook.com.	5	IN	CNAME	www.facebook.com.
www.facebook.com.	5	IN	CNAME	star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.	5	IN	A	31.13.75.35
afa.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
apps.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
asia.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
bc.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
beta.facebook.com.	5	IN	CNAME	latest.c10r.facebook.com.
latest.c10r.facebook.com.	5	IN	A	31.13.75.11
blog.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
c.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
citrix.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
d.facebook.com.	5	IN	CNAME	z-m.facebook.com.
z-m.facebook.com.	5	IN	CNAME	z-m.c10r.facebook.com.
z-m.c10r.facebook.com.	5	IN	A	31.13.75.36
development.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
dev.facebook.com.	5	IN	CNAME	intern-regional.vvv.facebook.com.
intern-regional.vvv.facebook.com.	5	IN	A	10.110.143.17
diplomatie.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
dns.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
es.facebook.com.	5	IN	CNAME	star.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
upload.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
web.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
w.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
webmail.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
www.facebook.com.	5	IN	CNAME	star-mini.c10r.facebook.com.
star-mini.c10r.facebook.com.	5	IN	A	31.13.75.35
www.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
ww.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1
www2.facebook.com.	5	IN	CNAME	star.facebook.com.
star.facebook.com.	5	IN	CNAME	star.c10r.facebook.com.
star.c10r.facebook.com.	5	IN	A	31.13.75.1

Facebook.com class C netranges:

31.13.75.0/24
69.171.251.0/24
129.134.30.0/24
129.134.31.0/24
185.89.218.0/24
185.89.219.0/24

Performing reverse lookup on 1536 ip addresses:

2.75.13.31.in-addr.arpa.	3600	IN	PTR	(
1.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-star-shv-02-hkt1.facebook.com.
3.75.13.31.in-addr.arpa.	3600	IN	PTR	(
4.75.13.31.in-addr.arpa.	3600	IN	PTR	(
5.75.13.31.in-addr.arpa.	3600	IN	PTR	(

6.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-stun-shv-02-hkt1.facebook.com.
9.75.13.31.in-addr.arpa.	3600	IN	PTR	(
7.75.13.31.in-addr.arpa.	3600	IN	PTR	(
8.75.13.31.in-addr.arpa.	3600	IN	PTR	(
10.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-dgw-shv-02-hkt1.facebook.com.
11.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-latest-shv-02-hkt1.facebook.com.
14.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-atlas-shv-02-hkt1.facebook.com.
17.75.13.31.in-addr.arpa.	3600	IN	PTR	(
18.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-z-p1-shv-02-hkt1.facebook.com.
15.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-secure-shv-02-hkt1.facebook.com.
16.75.13.31.in-addr.arpa.	3600	IN	PTR	(
21.75.13.31.in-addr.arpa.	3600	IN	PTR	(
19.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-mqtt-shv-02-hkt1.facebook.com.
22.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-extern-shv-02-hkt1.facebook.com.
25.75.13.31.in-addr.arpa.	3600	IN	PTR	(
26.75.13.31.in-addr.arpa.	3600	IN	PTR	(
33.75.13.31.in-addr.arpa.	3600	IN	PTR	(
35.75.13.31.in-addr.arpa.	3600	IN	PTR	(
34.75.13.31.in-addr.arpa.	3600	IN	PTR	(
37.75.13.31.in-addr.arpa.	3600	IN	PTR	(
36.75.13.31.in-addr.arpa.	3600	IN	PTR	(
40.75.13.31.in-addr.arpa.	3600	IN	PTR	(
39.75.13.31.in-addr.arpa.	3600	IN	PTR	(
41.75.13.31.in-addr.arpa.	3600	IN	PTR	(
42.75.13.31.in-addr.arpa.	3600	IN	PTR	(
48.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-mws-shv-02-hkt1.facebook.com.
49.75.13.31.in-addr.arpa.	3600	IN	PTR	(
52.75.13.31.in-addr.arpa.	3600	IN	PTR	(
53.75.13.31.in-addr.arpa.	3600	IN	PTR	wit-edge-shv-02-hkt1.facebook.com.
55.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-z-p3-shv-02-hkt1.facebook.com.
57.75.13.31.in-addr.arpa.	3600	IN	PTR	(
56.75.13.31.in-addr.arpa.	3600	IN	PTR	(
61.75.13.31.in-addr.arpa.	3600	IN	PTR	(
59.75.13.31.in-addr.arpa.	3600	IN	PTR	(
58.75.13.31.in-addr.arpa.	3600	IN	PTR	(
62.75.13.31.in-addr.arpa.	3600	IN	PTR	edgeray-shv-02-hkt1.facebook.com.
128.75.13.31.in-addr.arpa.	3600	IN	PTR	(
129.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-mws-l-shv-02-hkt1.facebook.com.
130.75.13.31.in-addr.arpa.	3600	IN	PTR	(
135.75.13.31.in-addr.arpa.	3600	IN	PTR	(
134.75.13.31.in-addr.arpa.	3600	IN	PTR	(
160.75.13.31.in-addr.arpa.	3600	IN	PTR	(
169.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-z-p4-shv-02-hkt1.facebook.com.
171.75.13.31.in-addr.arpa.	3600	IN	PTR	(
168.75.13.31.in-addr.arpa.	3600	IN	PTR	(
168.75.13.31.in-addr.arpa.	3600	IN	PTR	(
170.75.13.31.in-addr.arpa.	3600	IN	PTR	(
173.75.13.31.in-addr.arpa.	3600	IN	PTR	(
175.75.13.31.in-addr.arpa.	3600	IN	PTR	(
192.75.13.31.in-addr.arpa.	3600	IN	PTR	(
200.75.13.31.in-addr.arpa.	3600	IN	PTR	(
201.75.13.31.in-addr.arpa.	3600	IN	PTR	(
197.75.13.31.in-addr.arpa.	3600	IN	PTR	(
199.75.13.31.in-addr.arpa.	3600	IN	PTR	(
196.75.13.31.in-addr.arpa.	3600	IN	PTR	(
194.75.13.31.in-addr.arpa.	3600	IN	PTR	(
202.75.13.31.in-addr.arpa.	3600	IN	PTR	(
204.75.13.31.in-addr.arpa.	3600	IN	PTR	(
203.75.13.31.in-addr.arpa.	3600	IN	PTR	(
205.75.13.31.in-addr.arpa.	3600	IN	PTR	lert-api-shv-02-hkt1.facebook.com.
206.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-c2p-shv-02-hkt1.facebook.com.
207.75.13.31.in-addr.arpa.	3600	IN	PTR	(
210.75.13.31.in-addr.arpa.	3600	IN	PTR	(
217.75.13.31.in-addr.arpa.	3600	IN	PTR	(
214.75.13.31.in-addr.arpa.	3600	IN	PTR	(
211.75.13.31.in-addr.arpa.	3600	IN	PTR	(
215.75.13.31.in-addr.arpa.	3600	IN	PTR	(
218.75.13.31.in-addr.arpa.	3600	IN	PTR	(
213.75.13.31.in-addr.arpa.	3600	IN	PTR	(
216.75.13.31.in-addr.arpa.	3600	IN	PTR	(
212.75.13.31.in-addr.arpa.	3600	IN	PTR	(
208.75.13.31.in-addr.arpa.	3600	IN	PTR	(
219.75.13.31.in-addr.arpa.	3600	IN	PTR	dohproxy-shv-02-hkt1.facebook.com.
209.75.13.31.in-addr.arpa.	3600	IN	PTR	(
221.75.13.31.in-addr.arpa.	3600	IN	PTR	(
220.75.13.31.in-addr.arpa.	3600	IN	PTR	(
222.75.13.31.in-addr.arpa.	3600	IN	PTR	edge-x2p-shv-02-hkt1.facebook.com.
223.75.13.31.in-addr.arpa.	3600	IN	PTR	(
224.75.13.31.in-addr.arpa.	3600	IN	PTR	(
251.251.171.69.in-addr.arpa.	3600	IN	PTR	(
11.30.134.129.in-addr.arpa.	3600	IN	PTR	a.ns.c10r.facebook.com.
12.30.134.129.in-addr.arpa.	172800	IN	PTR	a.ns.facebook.com.
11.31.134.129.in-addr.arpa.	3600	IN	PTR	b.ns.c10r.facebook.com.
12.31.134.129.in-addr.arpa.	172800	IN	PTR	b.ns.facebook.com.
11.218.89.185.in-addr.arpa.	3600	IN	PTR	c.ns.c10r.facebook.com.
12.218.89.185.in-addr.arpa.	172800	IN	PTR	c.ns.facebook.com.
11.219.89.185.in-addr.arpa.	3600	IN	PTR	d.ns.c10r.facebook.com.
12.219.89.185.in-addr.arpa.	172800	IN	PTR	d.ns.facebook.com.

92 results out of 1536 IP addresses.

facebook.com ip blocks:

31.13.75.1/32
31.13.75.2/31
31.13.75.4/30
31.13.75.8/30
31.13.75.14/31
31.13.75.16/30
31.13.75.21/32
31.13.75.22/32
31.13.75.25/32
31.13.75.26/32
31.13.75.33/32
31.13.75.34/31
31.13.75.36/31
31.13.75.39/32
31.13.75.40/31
31.13.75.42/32
31.13.75.48/31
31.13.75.52/31
31.13.75.55/32
31.13.75.56/30
31.13.75.61/32
31.13.75.62/32
31.13.75.128/31
31.13.75.130/32
31.13.75.134/31
31.13.75.160/32
31.13.75.168/30
31.13.75.173/32
31.13.75.175/32
31.13.75.192/32
31.13.75.194/32
31.13.75.196/31
31.13.75.199/32
31.13.75.200/29
31.13.75.208/28
31.13.75.224/32
69.171.251.251/32
129.134.30.11/32
129.134.30.12/32
129.134.31.11/32
129.134.31.12/32
185.89.218.11/32
185.89.218.12/32
185.89.219.11/32
185.89.219.12/32

done.

- Sử dụng dnsrecon (thực hiện với 3 tên miền)

#dnsrecon -d ptit.edu.vn

1.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Thu Nov 9 08:03:43 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# dnsrecon -d dantri.com.vn
[*] std: Performing General Enumeration against: dantri.com.vn...
[*] Wildcard resolution is enabled on this domain
[*] It is resolving to 42.113.206.26
[*] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for dantri.com.vn
[*] SOA ns1.dantri.com.vn 42.113.206.23
[*] NS ns1.dantri.com.vn 42.113.206.23
[*] Bind Version for 42.113.206.23 "gdnssd/3"
[*] NS ns2.dantri.com.vn 125.212.194.153
[*] Bind Version for 125.212.194.153 "gdnssd/3"
[*] MX aspmx.l.google.com 173.194.174.27
[*] MX alt1.aspmx.l.google.com 142.250.141.27
[*] MX alt2.aspmx.l.google.com 142.250.115.26
[*] MX aspmx2.googlemail.com 142.250.141.26
[*] MX aspmx3.googlemail.com 142.250.115.27
[*] MX aspmx4.googlemail.com 64.233.171.27
[*] MX aspmx5.googlemail.com 142.250.152.26
[*] MX aspmx.l.google.com 2404:6800:4008:c1b::1a
[*] MX alt1.aspmx.l.google.com 2607:f8b0:4023:c0b::1b
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:1004::1b
[*] MX aspmx2.googlemail.com 2607:f8b0:4023:c0b::1b
[*] MX aspmx3.googlemail.com 2607:f8b0:4023:1004::1b
[*] MX aspmx4.googlemail.com 2607:f8b0:4003:c15::1b
[*] MX aspmx5.googlemail.com 2607:f8b0:4001:c56::1b
[*] A dantri.com.vn 42.113.206.26
[*] TXT dantri.com.vn google-site-verification=wgZVkoGePce2hVf5tRIAiCGbR1jXdHAHwtLI5J-xYnk
[*] TXT dantri.com.vn google-site-verification=AR12pmLT4sh8J6jAhZ77VeyHe4-S8MGzLNGcTYzvA50
[*] TXT dantri.com.vn amazonses:W0g/jEhQ9PiXV9NE5xt9C4wNWTwYWmuOnL9WZiwoe8o=
[*] TXT dantri.com.vn google-site-verification=B3CH6DBWp2M8Q8LDFMeWdLfCqQXbpoYdPOL_iteaxp0
[*] TXT dantri.com.vn google-site-verification=N5SXWp-2F54-jCNxCtLYkPEWf6M4COC2S2gQFdRbVI4
[*] Enumerating SRV Records
[-] No SRV Records Found for dantri.com.vn
```

2.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Thu Nov 9 08:05:24 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# dnsrecon -d facebook.com
[*] std: Performing General Enumeration against: facebook.com...
[-] DNSSEC is not configured for facebook.com
[*] SOA a.ns.facebook.com 129.134.30.12
[*] SOA a.ns.facebook.com 2a03:2880:f0fc:c:face:b00c:0:35
[*] NS a.ns.facebook.com 129.134.30.12
[*] NS a.ns.facebook.com 2a03:2880:f0fc:c:face:b00c:0:35
[*] NS b.ns.facebook.com 129.134.31.12
[*] NS b.ns.facebook.com 2a03:2880:f0fd:c:face:b00c:0:35
[*] NS c.ns.facebook.com 185.89.218.12
[*] NS c.ns.facebook.com 2a03:2880:f1fc:c:face:b00c:0:35
[*] NS d.ns.facebook.com 185.89.219.12
[*] NS d.ns.facebook.com 2a03:2880:f1fd:c:face:b00c:0:35
[*] MX smtpin.vvv.facebook.com 66.220.149.251
[*] MX smtpin.vvv.facebook.com 2a03:2880:ff:fffd:face:b00c:0:686e
[*] A facebook.com 31.13.75.35
[*] AAAA facebook.com 2a03:2880:f15a:181:face:b00c:0:25de
[*] TXT facebook.com google-site-verification=A2WZWCNQHrGV_TWwKh6KHY90tY0SHZo_RnyMJ0DaG0s
[*] TXT facebook.com v=spf1 redirect=spf.facebook.com
[*] TXT facebook.com google-site-verification=wdH5DTJtc9AYNwVunSVFeK0hYDGUIEOGb-RReU6pJlY
[*] TXT facebook.com google-site-verification=sK6uY9x7eaMoEMfn30ILqwTFYgaNp4lmgukI-C3_iA
[*] TXT facebook.com zoom-domain-verification=a6c90d61-66ec-485c-9f3d-cce7036f01bb
[*] TXT _dmarc.facebook.com v=DMARC1; p=reject; rua=mailto:a@dmARC.facebookmail.com; ruf=mailto:fb-dmarc@datafeeds.phishlabs.com; pct=100
[*] Enumerating SRV Records
[-] No SRV Records Found for facebook.com
```

3.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Thu Nov 9 08:06:16 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# dnsrecon -d google.com
[*] std: Performing General Enumeration against: google.com...
[-] DNSSEC is not configured for google.com
[*] SOA ns1.google.com 216.239.32.10
[*] SOA ns1.google.com 2001:4860:4802:32::a
[*] NS ns3.google.com 216.239.36.10
[*] NS ns3.google.com 2001:4860:4802:36::a
[*] NS ns2.google.com 216.239.34.10
[*] NS ns2.google.com 2001:4860:4802:34::a
[*] NS ns4.google.com 216.239.38.10
[*] NS ns4.google.com 2001:4860:4802:38::a
[*] NS ns1.google.com 216.239.32.10
[*] NS ns1.google.com 2001:4860:4802:32::a
[*] MX smtp.google.com 74.125.23.27
[*] MX smtp.google.com 74.125.203.27
[*] MX smtp.google.com 74.125.204.27
[*] MX smtp.google.com 64.233.187.26
[*] MX smtp.google.com 64.233.188.26
[*] MX smtp.google.com 2404:6800:4008:c02::1b
[*] MX smtp.google.com 2404:6800:4008:c03::1a
[*] MX smtp.google.com 2404:6800:4008:c04::1b
[*] MX smtp.google.com 2404:6800:4008:c05::1a
[*] A google.com 172.217.27.14
[*] AAAA google.com 2404:6800:4005:807::200e
[*] TXT google.com MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB
[*] TXT google.com webexdomainverification.8YX6G=6e6922db-e3e6-4a36-904e-a805c28087fa
[*] TXT google.com google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o
[*] TXT google.com google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cp0JM0nikft0jAgjmsQ
[*] TXT google.com onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef
[*] TXT google.com v=spf1 include:_spf.google.com ~all
[*] TXT google.com globalsign-smime-dv=CDYX+XFHw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8=
[*] TXT google.com docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e
[*] TXT google.com apple-domain-verification=30afIBcvSuDV2PLX
[*] TXT google.com docusign=1b0a6754-49b1-4db5-8540-d2c12664b289
[*] TXT google.com facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95
[*] TXT google.com atlassian-domain-verification=5YjTmWmjI92ewqkx2oXmBaD60Td9zWon9r6eakvHX6B77zzkF
Qto8PQ9QsKnbf4I
[*] TXT _dmarc.google.com v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com
[*] Enumerating SRV Records

[*] Enumerating SRV Records
[+] SRV _ldap._tcp.google.com ldap.google.com 216.239.32.58 389
[+] SRV _ldap._tcp.google.com ldap.google.com 2001:4860:4802:32::3a 389
[+] SRV _carddavs._tcp.google.com google.com 142.251.130.14 443
[+] SRV _carddavs._tcp.google.com google.com 2404:6800:4005:807::200e 443
[+] SRV _caldavs._tcp.google.com calendar.google.com 142.250.207.78 443
[+] SRV _caldavs._tcp.google.com calendar.google.com 2404:6800:4005:820::200e 443
[+] SRV _caldav._tcp.google.com calendar.google.com 142.250.207.78 80
[+] SRV _caldav._tcp.google.com calendar.google.com 2404:6800:4005:820::200e 80
[+] 8 Records Found
```


- Sử dụng nmap (thực hiện với 3 tên miền)

#nmap -p53 -T4 --script dns-brute www.ptit.edu.vn

1.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Thu Nov 9 08:09:27 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# nmap -p53 -T4 --script dns-brute www.ptit.edu.vn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 08:10 +07
Nmap scan report for www.ptit.edu.vn (222.255.113.97)
Host is up (0.00049s latency).
rDNS record for 222.255.113.97: static.vnpt.vn

PORT      STATE      SERVICE
53/tcp    filtered  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     cdn.ptit.edu.vn - 222.255.113.97
|     www.ptit.edu.vn - 222.255.113.97
|_    mail.ptit.edu.vn - 123.30.182.167

Nmap done: 1 IP address (1 host up) scanned in 19.27 seconds
```

2.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Thu Nov 9 08:11:00 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# nmap -p53 -T4 --script dns-brute www.dantri.com.vn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 08:11 +07
Nmap scan report for www.dantri.com.vn (42.113.206.26)
Host is up (0.00088s latency).

PORT      STATE      SERVICE
53/tcp    filtered  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     ads.dantri.com.vn - 42.113.206.9
|     test.dantri.com.vn - 42.113.206.59
|     ns1.dantri.com.vn - 42.113.206.23
|     ns2.dantri.com.vn - 125.212.194.153
|     app.dantri.com.vn - 151.101.1.195
|     app.dantri.com.vn - 151.101.65.195
|     ftp.dantri.com.vn - 42.113.206.12
|     beta.dantri.com.vn - 42.113.206.59
|     cms.dantri.com.vn - 192.168.13.10
|     demo.dantri.com.vn - 42.113.206.59
|_    *A: 42.113.206.26

Nmap done: 1 IP address (1 host up) scanned in 10.46 seconds
```

3.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Thu Nov 9 08:11:47 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# nmap -p53 -T4 --script dns-brute www.facebook.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 08:11 +07
Nmap scan report for www.facebook.com (31.13.75.35)
Host is up (0.0014s latency).
Other addresses for www.facebook.com (not scanned): 2a03:2880:f15a:181:face:b00c:0:25de
rDNS record for 31.13.75.35: edge-star-mini-shv-02-hkt1.facebook.com

PORT      STATE      SERVICE
53/tcp    filtered  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|   development.facebook.com - 31.13.75.1
|   development.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   ads.facebook.com - 31.13.75.35
|   ads.facebook.com - 2a03:2880:f15a:181:face:b00c::25de
|   mysql.facebook.com - 31.13.75.1
|   mysql.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   news.facebook.com - 31.13.75.1
|   news.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   ns.facebook.com - 31.13.75.1
|   ns.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   upload.facebook.com - 31.13.75.1
|   dns.facebook.com - 31.13.75.1
|   upload.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   dns.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   alpha.facebook.com - 31.13.75.11
|   alpha.facebook.com - 2a03:2880:f05a:10a:face:b00c::4f5a
|   web.facebook.com - 31.13.75.1
|   web.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   apps.facebook.com - 31.13.75.1
|   apps.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   secure.facebook.com - 31.13.75.15
|   www.facebook.com - 31.13.75.35
|   www.facebook.com - 2a03:2880:f15a:181:face:b00c::25de
|   secure.facebook.com - 2a03:2880:f05a:10e:face:b00c::2b80
|   www2.facebook.com - 31.13.75.1
|   www2.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|
|   www2.facebook.com - 31.13.75.1
|   www2.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   shop.facebook.com - 31.13.75.1
|   shop.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   beta.facebook.com - 31.13.75.11
|   beta.facebook.com - 2a03:2880:f05a:10a:face:b00c::4f5a
|   blog.facebook.com - 31.13.75.1
|   blog.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   mobile.facebook.com - 31.13.75.1
|   mobile.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   citrix.facebook.com - 31.13.75.1
|   citrix.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   ssl.facebook.com - 31.13.75.1
|   ssl.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   crs.facebook.com - 31.13.75.1
|   crs.facebook.com - 2a03:2880:f05a:110:face:b00c::2
|   dev.facebook.com - 10.110.231.12
|   dev.facebook.com - 2401:db00:10ff:ff34:face:b00c::75c6
|_

Nmap done: 1 IP address (1 host up) scanned in 4.97 seconds
```

```

(root@B20AT094-Huong-Kali)-[/home/huong-at094] /homepage.html
# date
Thu Nov 9 08:14:27 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# nmap -p53 -T4 --script dns-brute www.google.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-09 08:14 +07
Nmap scan report for www.google.com (142.251.220.4)
Host is up (0.00044s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4005:80c::2004
rDNS record for 142.251.220.4: hkg07s49-in-f4.1e100.net

PORT      STATE      SERVICE
53/tcp    filtered  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     admin.google.com - 216.58.203.78
|     admin.google.com - 2404:6800:4005:80a::200e
|     ads.google.com - 142.251.220.14
|     id.google.com - 172.217.27.3
|     id.google.com - 2404:6800:4005:802::2003
|     ads.google.com - 2404:6800:4005:80c::200e
|     images.google.com - 142.250.207.78
|     images.google.com - 2404:6800:4005:820::200e
|     alerts.google.com - 142.250.204.110
|     alerts.google.com - 2404:6800:4005:814::200e
|     ap.google.com - 172.217.27.4
|     ap.google.com - 2404:6800:4005:807::2004
|     dns.google.com - 8.8.4.4
|     dns.google.com - 8.8.8.8
|     dns.google.com - 2001:4860:4860::8844
|     dns.google.com - 2001:4860:4860::8888
|     apps.google.com - 142.250.204.110
|     ipv6.google.com - 2404:6800:4005:802::200e
|     apps.google.com - 2404:6800:4005:814::200e
|     news.google.com - 142.250.207.78
|     ldap.google.com - 216.239.32.58
|     download.google.com - 172.217.27.4
|     news.google.com - 2404:6800:4005:820::200e
|     ldap.google.com - 2001:4860:4802:32::3a
|     download.google.com - 2404:6800:4005:807::2004
|     ns.google.com - 216.239.32.10
|     local.google.com - 142.250.204.46
|     local.google.com - 2404:6800:4005:812::200e
|     upload.google.com - 142.251.220.111
|     upload.google.com - 2404:6800:4005:80f::200f
|     ns1.google.com - 216.239.32.10
|     mail.google.com - 172.217.27.37
|     ns1.google.com - 2001:4860:4802:32::a
|     mail.google.com - 2404:6800:4005:808::2005
|     ns2.google.com - 216.239.34.10
|     ns2.google.com - 2001:4860:4802:34::a
|     ns3.google.com - 216.239.36.10
|     ns3.google.com - 2001:4860:4802:36::a
|     vpn.google.com - 64.9.224.68
|     vpn.google.com - 64.9.224.69
|     vpn.google.com - 64.9.224.70
|     web.google.com - 142.250.204.110
|     web.google.com - 2404:6800:4005:814::200e
|     whois.google.com - 216.239.34.22
|     blog.google.com - 172.217.24.105
|     whois.google.com - 2001:4860:4802:34::16
|     blog.google.com - 2404:6800:4005:800::2009
|     mobile.google.com - 216.58.203.75
|     mobile.google.com - 2404:6800:4005:80a::200b
|     chat.google.com - 142.251.220.14
|     www.google.com - 142.251.220.4
|     www.google.com - 2404:6800:4005:80c::2004
|     chat.google.com - 2404:6800:4005:80c::200e
|     help.google.com - 142.250.204.110
|     help.google.com - 2404:6800:4005:814::200e
|     corp.google.com - 64.233.188.129
|     corp.google.com - 2404:6800:4008:c06::81
|     smtp.google.com - 64.233.187.26
|     smtp.google.com - 64.233.188.27
|     smtp.google.com - 74.125.203.27
|     smtp.google.com - 74.125.204.26
|     smtp.google.com - 74.125.23.26
|     smtp.google.com - 2404:6800:4008:c02::1b
|     smtp.google.com - 2404:6800:4008:c03::1b
|     smtp.google.com - 2404:6800:4008:c04::1b
|     smtp.google.com - 2404:6800:4008:c05::1a
|     home.google.com - 142.251.220.14
|     home.google.com - 2404:6800:4005:80c::200e

Nmap done: 1 IP address (1 host up) scanned in 8.85 seconds

```