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 Hướng

**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

# An toàn mạng (INT1482) - Bài thực hành số 1

## 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:
  o nslookup
  o dig
  o dnsenum
  o dnsrecon
  o 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 ❼ IP và ngược lại. Thông tin về các tên miền được lưu trong các file gọi là zone (vùng/miền).
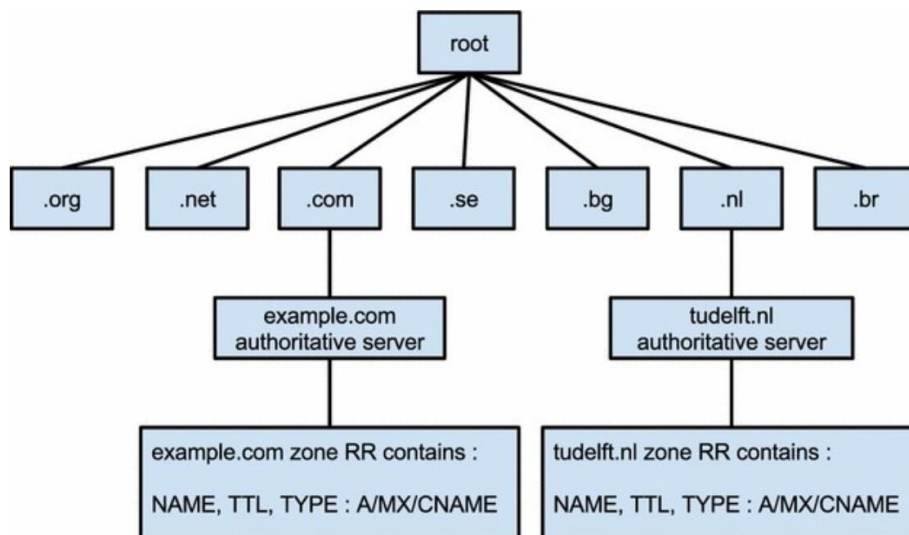
# 3. Nội dung thực hành

## 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
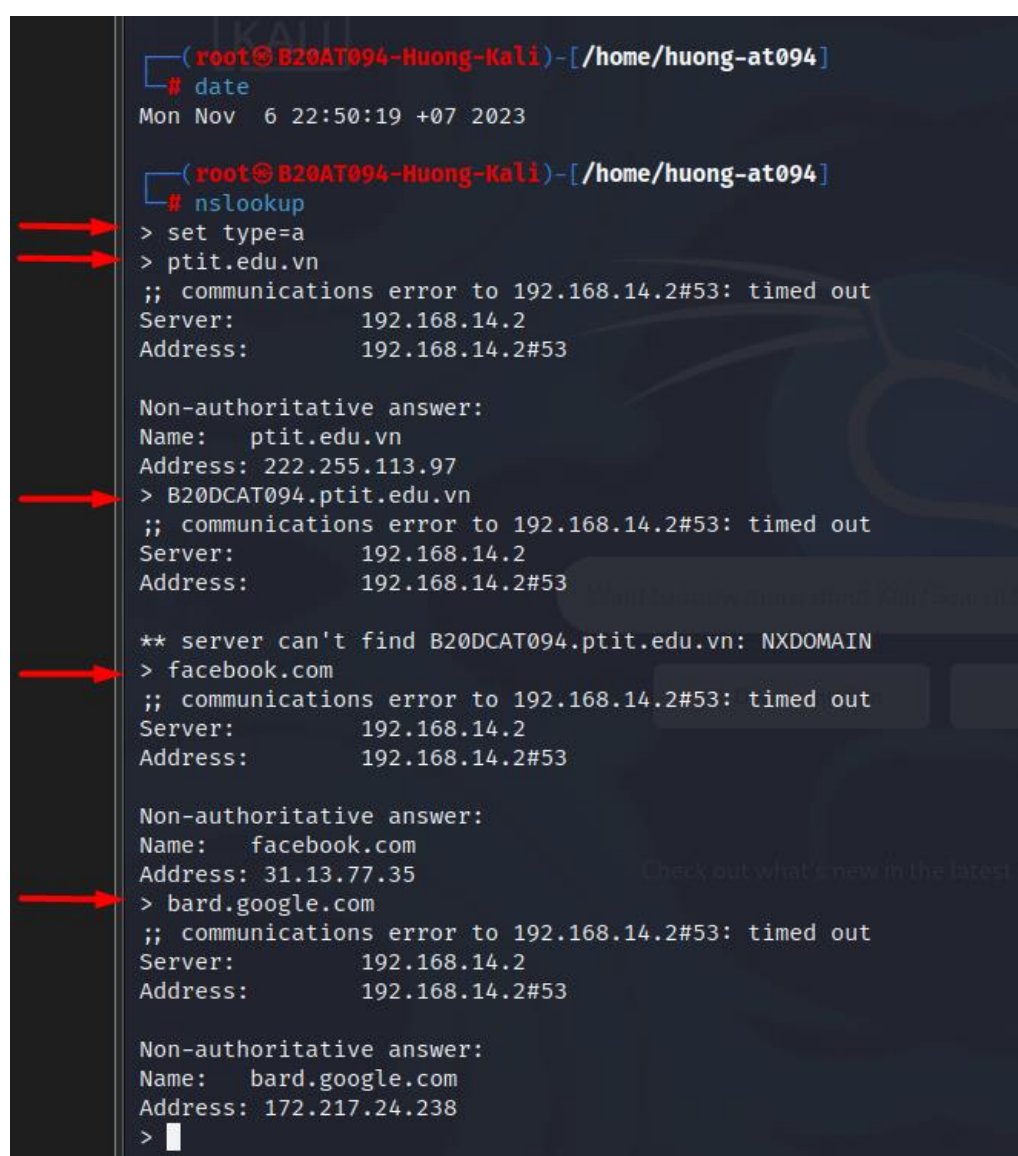
## 3.2 Tìm thông tin về tên miền sử dụng nslookup

- 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



3

- 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

- Tìm tên miền tương ứng với địa chỉ IP (thực hiện với 3 địa chỉ IP)
>set type = ptr
>64.233.187.26

## 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: 0×0005, 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]
└─#
```

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

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: 0×0005, udp: 512
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.            5        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: 0×0005, udp: 512
;; QUESTION SECTION:
;facebook.com.                  IN      A

;; ANSWER SECTION:
facebook.com.          5        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)

<mark>#dnsenum --thread 15 -s ptit.edu.vn</mark>

1.

```
┌──(root☠B20AT094-Huong-Kali)-[/home/huong-at094]
└─# date
Thu Nov  9 07:54:21 +07 2023

┌──(root☠B20AT094-Huong-Kali)-[/home/huong-at094]
└─# dnsenum --thread 15 -s ptit.edu.vn
dnsenum VERSION:1.2.6
Unknown option: –thread
Value "ptit.edu.vn" invalid for option s (number expected)


─────    15    ─────


Host's addresses:
_____



Name Servers:
_____

y.arin.net.                               5        IN    A     192.82.134.30
u.arin.net.                               5        IN    A     204.61.216.50
z.arin.net.                               5        IN    A     199.180.180.63
r.arin.net.                               5        IN    A     199.180.180.63
arin.authdns.ripe.net.                    5        IN    A     193.0.9.10
x.arin.net.                               5        IN    A     199.180.180.63


Mail (MX) Servers:
_____



Trying Zone Transfers and getting Bind Versions:
_____


Trying Zone Transfer for 15 on y.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on u.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on z.arin.net ...
AXFR record query failed: REFUSED
```

```
Trying Zone Transfer for 15 on x.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on u.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on z.arin.net ...
AXFR record query failed: REFUSED


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

9

2.

```
┌──(root💀B20AT094-Huong-Kali)-[/home/huong-at094]
└─# date
Thu Nov  9 07:56:30 +07 2023

┌──(root💀B20AT094-Huong-Kali)-[/home/huong-at094]
└─# dnsenum --thread 15 -s dantri.com.vn
dnsenum VERSION:1.2.6
Unknown option: --thread
Value "dantri.com.vn" invalid for option s (number expected)


─────    15    ─────


Host's addresses:
_____



Name Servers:
_____


u.arin.net.                                5        IN    A    204.61.216.50
y.arin.net.                                5        IN    A    192.82.134.30
x.arin.net.                                5        IN    A    199.180.180.63
z.arin.net.                                5        IN    A    199.180.180.63
r.arin.net.                                5        IN    A    199.180.180.63
arin.authdns.ripe.net.                     5        IN    A    193.0.9.10


Mail (MX) Servers:
_____



Trying Zone Transfers and getting Bind Versions:
_____


Trying Zone Transfer for 15 on u.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on y.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on x.arin.net ...
AXFR record query failed: REFUSED
```

3.

```
┌──(root㊙B20AT094-Huong-Kali)-[/home/huong-at094]
└─# date
Thu Nov  9 08:00:32 +07 2023

┌──(root㊙B20AT094-Huong-Kali)-[/home/huong-at094]
└─# dnsenum --thread 15 -s facebook.com
dnsenum VERSION:1.2.6
Unknown option: —thread
Value "facebook.com" invalid for option s (number expected)


——   15   ——


Host's addresses:
_____



Name Servers:
_____


y.arin.net.                             5        IN    A     192.82.134.30
z.arin.net.                             5        IN    A     199.180.180.63
u.arin.net.                             5        IN    A     204.61.216.50
r.arin.net.                             5        IN    A     199.180.180.63
x.arin.net.                             5        IN    A     199.180.180.63
arin.authdns.ripe.net.                  5        IN    A     193.0.9.10


Mail (MX) Servers:
_____



Trying Zone Transfers and getting Bind Versions:
_____


Trying Zone Transfer for 15 on y.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on z.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on u.arin.net ...
AXFR record query failed: REFUSED
```

4.

```
  ┌──(root💀B20AT094-Huong-Kali)-[/home/huong-at094]
  └─# date
Thu Nov  9 08:02:25 +07 2023

  ┌──(root💀B20AT094-Huong-Kali)-[/home/huong-at094]
  └─# dnsenum --thread 15 -s viblo.asia
dnsenum VERSION:1.2.6
Unknown option: --thread
Value "viblo.asia" invalid for option s (number expected)


 ──────     15     ──────


Host's addresses:
_____



Name Servers:
_____

arin.authdns.ripe.net.                       5         IN    A        193.0.9.10
y.arin.net.                                   5         IN    A        192.82.134.30
x.arin.net.                                   5         IN    A        199.180.180.63
u.arin.net.                                   5         IN    A        204.61.216.50
z.arin.net.                                   5         IN    A        199.180.180.63
r.arin.net.                                   5         IN    A        199.180.180.63


Mail (MX) Servers:
_____



Trying Zone Transfers and getting Bind Versions:
_____


Trying Zone Transfer for 15 on arin.authdns.ripe.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on y.arin.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for 15 on x.arin.net ...
AXFR record query failed: REFUSED
```

12

- 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 "gdnsd/3"
[*]      NS ns2.dantri.com.vn 125.212.194.153
[*]      Bind Version for 125.212.194.153 "gdnsd/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:WOg/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

┌──(root💀B20AT094-Huong-Kali)-[/home/huong-at094]
└─#
```

13

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_RnyMJoDaG0s
[*]      TXT facebook.com v=spf1 redirect=_spf.facebook.com
[*]      TXT facebook.com google-site-verification=wdH5DTJTc9AYNwVunSVFeK0hYDGUIEOGb-RReU6pJlY
[*]      TXT facebook.com google-site-verification=sK6uY9×7eaMoEMfn3OILqwTFYgaNp4llmguKI-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_J9cpOJM0nikft0jAgjmsQ
[*]      TXT google.com onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef
[*]      TXT google.com v=spf1 include:_spf.google.com ~all
[*]      TXT google.com globalsign-smime-dv=CDYX+XFHUw2wml6/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
```

4.

```
┌──(root💀B20AT094-Huong-Kali)-[/home/huong-at094]
└─# 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
```