

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



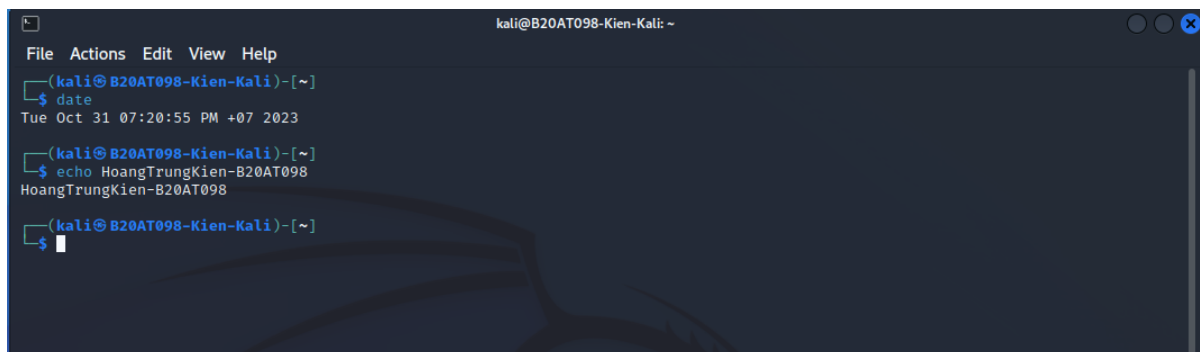
MÔN HỌC: AN TOÀN MẠNG
BÁO CÁO THỰC HÀNH BÀI 1

Giảng viên: Hoàng Xuân Dậu

Sinh viên: Hoàng Trung Kiên – B20DCAT098

Hà Nội – 11/2023

1. Đổi tên máy kali



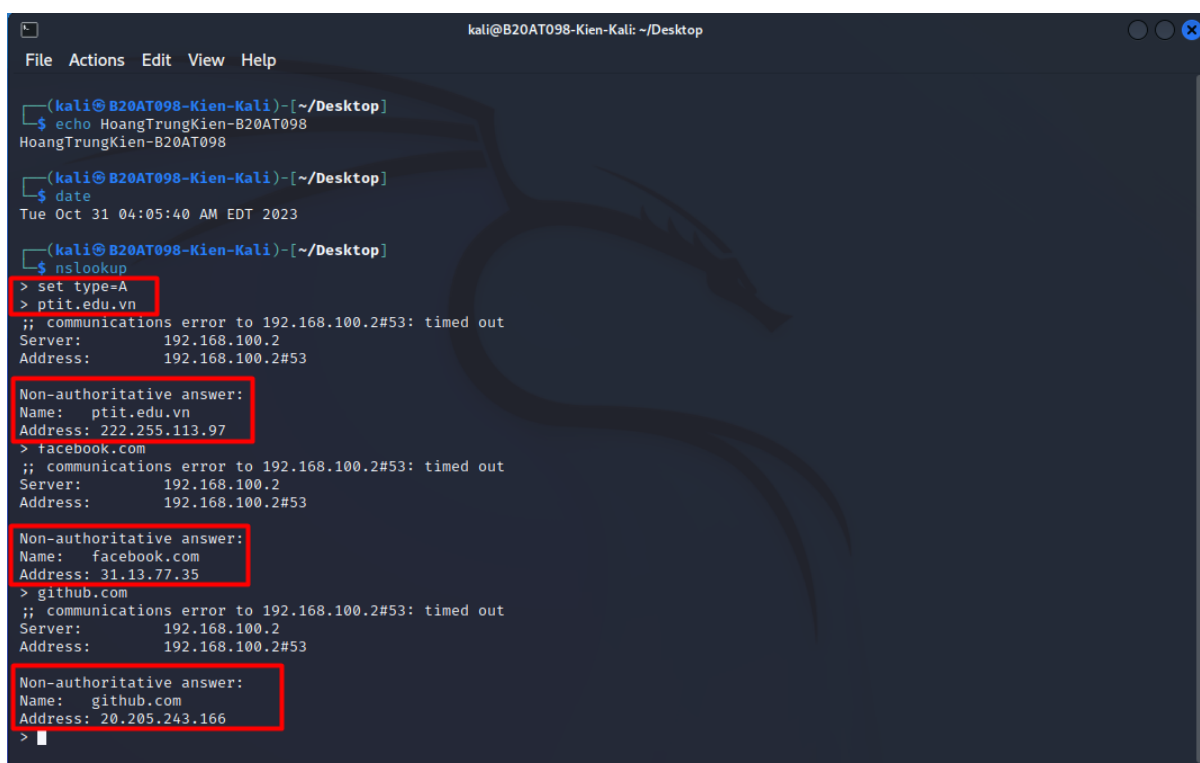
```
kali@B20AT098-Kien-Kali: ~  
File Actions Edit View Help  
(kali@B20AT098-Kien-Kali)-[~]  
$ date  
Tue Oct 31 07:20:55 PM +07 2023  
(kali@B20AT098-Kien-Kali)-[~]  
$ echo HoangTrungKien-B20AT098  
HoangTrungKien-B20AT098  
(kali@B20AT098-Kien-Kali)-[~]  
$
```

2. Thực hành

a, Tìm thông tin về tên miền sử dụng nslookup

Khởi động nslookup trong cửa sổ terminal

- Tìm địa chỉ IP của các tên miền



```
kali@B20AT098-Kien-Kali: ~/Desktop  
File Actions Edit View Help  
(kali@B20AT098-Kien-Kali)-[~/Desktop]  
$ echo HoangTrungKien-B20AT098  
HoangTrungKien-B20AT098  
(kali@B20AT098-Kien-Kali)-[~/Desktop]  
$ date  
Tue Oct 31 04:05:40 AM EDT 2023  
(kali@B20AT098-Kien-Kali)-[~/Desktop]  
$ nslookup  
> set type=A  
> ptit.edu.vn  
;; communications error to 192.168.100.2#53: timed out  
Server: 192.168.100.2  
Address: 192.168.100.2#53  
  
Non-authoritative answer:  
Name: ptit.edu.vn  
Address: 222.255.113.97  
> facebook.com  
;; communications error to 192.168.100.2#53: timed out  
Server: 192.168.100.2  
Address: 192.168.100.2#53  
  
Non-authoritative answer:  
Name: facebook.com  
Address: 31.13.77.35  
> github.com  
;; communications error to 192.168.100.2#53: timed out  
Server: 192.168.100.2  
Address: 192.168.100.2#53  
  
Non-authoritative answer:  
Name: github.com  
Address: 20.205.243.166  
>
```

- Tìm máy chủ DNS của các tên miền

```

(kali@B20AT098-Kien-Kali)-[~/Desktop]
$ date
Tue Oct 31 04:07:57 AM EDT 2023

(kali@B20AT098-Kien-Kali)-[~/Desktop]
$ echo HoangTrungKien-B20AT098
HoangTrungKien-B20AT098

(kali@B20AT098-Kien-Kali)-[~/Desktop]
$ nslookup
> set type=NS
> ptit.edu.vn
;; communications error to 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#53

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

Authoritative answers can be found from:
> facebook.com
;; communications error to 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#53

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

Authoritative answers can be found from:
> github.com
;; communications error to 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#53

Non-authoritative answer:
github.com  nameserver = ns-1283.awsdns-32.org.
github.com  nameserver = dns2.p08.nsone.net.
github.com  nameserver = ns-1707.awsdns-21.co.uk.
github.com  nameserver = dns1.p08.nsone.net.

```

- Tìm máy chủ email của các tên miền

```

> set type=mx
> ptit.edu.vn
;; communications error to 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#53

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

Authoritative answers can be found from:
> facebook.com
;; communications error to 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#53

Non-authoritative answer:
facebook.com mail exchanger = 10 smtpin.vvv.facebook.com.

Authoritative answers can be found from:
> github.com
;; communications error to 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#53

Non-authoritative answer:
github.com  mail exchanger = 10 alt4.aspmx.l.google.com.
github.com  mail exchanger = 1 aspmx.l.google.com.
github.com  mail exchanger = 10 alt3.aspmx.l.google.com.
github.com  mail exchanger = 5 alt2.aspmx.l.google.com.
github.com  mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
>

```

- Tìm tên miền tương ứng với địa chỉ IP

```
kali@B20AT098-Kien-Kali: ~/Desktop
File Actions Edit View Help
(kali@B20AT098-Kien-Kali)~[~/Desktop]
$ date
Tue Oct 31 04:14:52 AM EDT 2023

(kali@B20AT098-Kien-Kali)~[~/Desktop]
$ nslookup
> set type PTR
> 64.233.187.26
;; communications error to 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#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 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#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 192.168.100.2#53: timed out
Server:      192.168.100.2
Address:     192.168.100.2#53

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

Authoritative answers can be found from:
>
```

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

Trang ptit.edu.vn

```
kali@B20AT098-Kien-Kali: ~
File Actions Edit View Help
(kali@B20AT098-Kien-Kali)~[~]
$ date
Tue Nov 7 01:15:03 PM +07 2023

(kali@B20AT098-Kien-Kali)~[~]
$ dig ptit.edu.vn

; <<>> DiG 9.18.8-1-Debian <<>> ptit.edu.vn
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 45220
;; 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: 12 msec
;; SERVER: 192.168.100.2#53(192.168.100.2) (UDP)
;; WHEN: Tue Nov 07 13:15:11 +07 2023
;; MSG SIZE rcvd: 56
```

```
(kali@B20AT098-Kien-Kali)-[~]
$ dnsenum ptit.edu.vn
dnsenum VERSION:1.2.6
```

ptit.edu.vn

Host's addresses:

ptit.edu.vn.	5	IN	A	222.255.113.97
--------------	---	----	---	----------------

Name Servers:

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

Mail (MX) Servers:

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

Trying Zone Transfers and getting Bind Versions:

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

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

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

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	CNAME	autod.ms-acdc-autod.office.com.
autod.ms-acdc-autod.office.com.	5	IN	A	52.98.50.24
autod.ms-acdc-autod.office.com.	5	IN	A	52.98.40.40
autod.ms-acdc-autod.office.com.	5	IN	A	40.100.55.8
autod.ms-acdc-autod.office.com.	5	IN	A	52.98.71.56
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
222.255.113.0/24

Performing reverse lookup on 768 ip addresses:

0 results out of 768 IP addresses.

ptit.edu.vn ip blocks:

done.

```

(kali@B20AT098-Kien-Kali)-[~]
$ dnsrecon -d ptit.edu.vn
[*] std: Performing General Enumeration against: ptit.edu.vn...
[-] DNSSEC is not configured for ptit.edu.vn
[*] SOA ns1.vdconline.vn 14.225.24.83
[*] NS ns1.vdconline.vn 14.225.24.83
[-] Recursion enabled on NS Server 14.225.24.83
[*] Bind Version for 14.225.24.83 ""
[*] NS ns2.vdconline.vn 14.225.24.84
[-] Recursion enabled on NS Server 14.225.24.84
[*] Bind Version for 14.225.24.84 ""
[*] MX ptit-edu-vn.mail.eo.outlook.com 52.101.132.28
[*] MX ptit-edu-vn.mail.eo.outlook.com 52.101.137.0
[*] MX ptit-edu-vn.mail.eo.outlook.com 52.101.132.30
[*] MX ptit-edu-vn.mail.eo.outlook.com 52.101.137.2
[*] A ptit.edu.vn 222.255.113.97
[*] TXT ptit.edu.vn MS=26A8D3D7EF33F0A2C8F64830DA0623FC9FD849F3
[*] TXT ptit.edu.vn v=spf1 include:spf.protection.outlook.com -all
[*] TXT ptit.edu.vn GS1g+fLBM5YvAfz2Ls/wmSyc5a/UeFFV71r1NWcB9K0HUojC4mXq5Qm3SYMvkIChsYyIaOuK2cGEauibjnMH8g==
[*] TXT ptit.edu.vn google-site-verification=FWkI061D2ztUTO-sXxdmFBfaJYALm5cz9G3WMQuUvAk
[*] Enumerating SRV Records
[+] 0 Records Found

(kali@B20AT098-Kien-Kali)-[~]
$ date
Tue Nov 7 01:16:20 PM +07 2023

```

```

(kali@B20AT098-Kien-Kali)-[~]
$ nmap -p53 -T4 --script dns-brute www.ptit.edu.vn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-07 13:16 +07
Nmap scan report for www.ptit.edu.vn (222.255.113.97)
Host is up (0.025s 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:
|     mail.ptit.edu.vn - 123.30.182.167
|     cdn.ptit.edu.vn - 222.255.113.97
|_    www.ptit.edu.vn - 222.255.113.97

Nmap done: 1 IP address (1 host up) scanned in 3.21 seconds

(kali@B20AT098-Kien-Kali)-[~]
$ date
Tue Nov 7 01:17:10 PM +07 2023

```

Trang web kenh14.vn

```

kali@B20AT098-Kien-Kali: ~
File Actions Edit View Help

(kali@B20AT098-Kien-Kali)-[~]
$ date
Tue Oct 31 07:24:25 PM +07 2023

(kali@B20AT098-Kien-Kali)-[~]
$ dig kenh14.vn

; <<>> DiG 9.18.8-1-Debian <<>> kenh14.vn
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 47913
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;kenh14.vn.                IN      A

;; ANSWER SECTION:
kenh14.vn.                 5       IN      A      14.225.199.133

;; Query time: 95 msec
;; SERVER: 192.168.100.2#53(192.168.100.2) (UDP)
;; WHEN: Tue Oct 31 19:24:56 +07 2023
;; MSG SIZE rcvd: 54

```



```

kali@B20AT098-Kien-Kali: ~
File Actions Edit View Help
~/Desktop
~/etc/hostname

(kali@B20AT098-Kien-Kali)-[~]
$ dnsrecon -d kenh14.vn
[*] std: Performing General Enumeration against: kenh14.vn...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 222.255.27.49
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for kenh14.vn
[*] SOA ns6.synerfy.vn 169.62.159.227
[*] NS ns6.synerfy.vn 169.62.159.227
[*] Bind Version for 169.62.159.227 "gdnssd"
[*] NS ns8.synerfy.vn 210.245.87.125
[*] Bind Version for 210.245.87.125 "gdnssd"
[*] NS ns7.synerfy.vn 123.30.51.247
[*] Bind Version for 123.30.51.247 "gdnssd"
[*] MX aspmx3.googlemail.com 142.250.115.27
[*] MX aspmx5.googlemail.com 142.250.152.26
[*] MX aspmx2.googlemail.com 142.250.141.27
[*] MX aspmx4.googlemail.com 64.233.171.26
[*] MX aspmx.l.google.com 173.194.174.27
[*] MX alt2.aspmx.l.google.com 142.250.115.26
[*] MX alt1.aspmx.l.google.com 142.250.141.27
[*] MX aspmx3.googlemail.com 2607:f8b0:4023:1004::1b
[*] MX aspmx5.googlemail.com 2607:f8b0:4001:c56::1b
[*] MX aspmx2.googlemail.com 2607:f8b0:4023:c0b::1a
[*] MX aspmx4.googlemail.com 2607:f8b0:4003:c15::1b
[*] MX aspmx.l.google.com 2404:6800:4008:c03::1a
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:1004::1a
[*] MX alt1.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*] A kenh14.vn 14.225.199.133
[*] TXT kenh14.vn v=spf1 include:spf.google.com ~all
[*] TXT kenh14.vn google-site-verification=84d_-5-q2bMy17aJwL4fGcu18owKk0Gns0kSIFymrys
[*] TXT kenh14.vn google-site-verification=05uAxb6-5wj3gR-2eYUpFxC1YKb99JBf0kc95kcxqYU
[*] TXT _dmarc.kenh14.vn v=DMARC1; p=quarantine; pct=100; rua=mailto:thanhtq@kenh14.vn
[*] Enumerating SRV Records
[+] 0 Records Found

(kali@B20AT098-Kien-Kali)-[~]
$ date
Tue Oct 31 07:39:47 PM +07 2023

```

```

(kali@B20AT098-Kien-Kali)-[~]
$ nmap -p53 -T4 --script dns-brute www.kenh14.vn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 19:40 +07
Nmap scan report for www.kenh14.vn (14.225.199.133)
Host is up (0.023s latency).
rDNS record for 14.225.199.133: static.vnpt.vn

PORT      STATE      SERVICE
53/tcp    filtered  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|   app.kenh14.vn - 123.30.151.82
|   app.kenh14.vn - 14.225.10.15
|   mail.kenh14.vn - 142.251.220.115
|   mail.kenh14.vn - 2404:6800:4005:811::2013
|   www.kenh14.vn - 14.225.199.133
|   *A: 222.255.27.49
Nmap done: 1 IP address (1 host up) scanned in 28.34 seconds

(kali@B20AT098-Kien-Kali)-[~]
$ date
Tue Oct 31 07:44:24 PM +07 2023

```


Trang web genk

[illegible]

Mail (MX) Servers:

```
aspmx5.googlemail.com. 5 IN A 142.250.152.26
alt2.aspmx.l.google.com. 5 IN A 142.250.115.27
aspmx2.googlemail.com. 5 IN A 142.250.141.27
alt1.aspmx.l.google.com. 5 IN A 142.250.141.26
aspmx3.googlemail.com. 5 IN A 142.250.115.27
aspmx4.googlemail.com. 5 IN A 64.233.171.27
aspmx.l.google.com. 5 IN A 108.177.97.27
```

Trying Zone Transfers and getting Bind Versions:

```
Trying Zone Transfer for genk.vn on ns6.synerfy.vn ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for genk.vn on ns8.synerfy.vn ...
AXFR record query failed: NOTIMP

Trying Zone Transfer for genk.vn on ns7.synerfy.vn ...
AXFR record query failed: NOTIMP
```

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

```
c.genk.vn. 5 IN A 123.30.151.94
mail.genk.vn. 5 IN CNAME ghs.google.com.
ghs.google.com. 5 IN A 142.251.220.51
www.genk.vn. 5 IN CNAME genk.vn.
genk.vn. 5 IN A 14.225.199.134
```

genk.vn class C netranges:

```
14.225.199.0/24
123.30.151.0/24
```

Performing reverse lookup on 512 ip addresses:

0 results out of 512 IP addresses.

genk.vn ip blocks:

```
done.
(kali@B20AT098-Kien-Kali)-[~]
$
(kali@B20AT098-Kien-Kali)-[~]
$
(kali@B20AT098-Kien-Kali)-[~]
$ date
Tue Oct 31 07:59:29 PM +07 2023
```

```

(kali@B20AT098-Kien-Kali)-[~]
$ date
Tue Oct 31 07:59:29 PM +07 2023

(kali@B20AT098-Kien-Kali)-[~]
$ dnsrecon -d genk.vn
[*] std: Performing General Enumeration against: genk.vn...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 222.255.27.49
[!] All queries will resolve to this list of addresses!!
[!] DNSSEC is not configured for genk.vn
[*] SOA ns8.synerfy.vn 210.245.87.125
[*] NS ns7.synerfy.vn 123.30.51.247
[*] Bind Version for 123.30.51.247 "gdnisd"
[*] NS ns6.synerfy.vn 169.62.159.227
[*] Bind Version for 169.62.159.227 "gdnisd"
[*] NS ns8.synerfy.vn 210.245.87.125
[*] Bind Version for 210.245.87.125 "gdnisd"
[*] MX aspmx2.googlemail.com 142.250.141.26
[*] MX alt1.aspmx.l.google.com 142.250.141.26
[*] MX aspmx5.googlemail.com 142.250.152.26
[*] MX aspmx.l.google.com 74.125.204.27
[*] MX aspmx4.googlemail.com 64.233.171.26
[*] MX alt2.aspmx.l.google.com 142.250.115.27
[*] MX aspmx3.googlemail.com 142.250.115.26
[*] MX aspmx2.googlemail.com 2607:f8b0:4023:c0b::1b
[*] MX alt1.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*] MX aspmx5.googlemail.com 2607:f8b0:4001:c56::1a
[*] MX aspmx.l.google.com 2404:6800:4008:c1b::1b
[*] MX aspmx4.googlemail.com 2607:f8b0:4003:c15::1a
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:1004::1b
[*] MX aspmx3.googlemail.com 2607:f8b0:4023:1004::1b
[*] A genk.vn 14.225.199.134
[*] TXT genk.vn v=spf1 include:_spf.google.com ~all
[*] TXT genk.vn google-site-verification=jLLyZmCG5FFtHcMUCekbgNtgtKG6gI66MjeiAdfZia8
[*] TXT _dmarc.genk.vn v=DMARC1; p=quarantine; pct=100; rua=mailto:thanhtq@genk.vn
[*] Enumerating SRV Records
[+] 0 Records Found

```

```

(kali@B20AT098-Kien-Kali)-[~]
$ nmap -p53 -T4 --script dns-brute www.genk.vn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 20:00 +07
Nmap scan report for www.genk.vn (14.225.199.134)
Host is up (0.024s latency).
rDNS record for 14.225.199.134: static.vnpt.vn
PORT      STATE      SERVICE
53/tcp    filtered  domain
Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|   mail.genk.vn - 216.58.200.243
|   mail.genk.vn - 2404:6800:4005:80d::2013
|   app.genk.vn - 123.30.151.74
|   www.genk.vn - 14.225.199.134
|_  *A: 222.255.27.49
Nmap done: 1 IP address (1 host up) scanned in 53.09 seconds

```

```

(kali@B20AT098-Kien-Kali)-[~]
$ date
Tue Oct 31 08:01:17 PM +07 2023

```

```

(kali@B20AT098-Kien-Kali)-[~]
$

```