

Báo cáo LAB 1+2

Information Gathering

Nhóm 11

22520037	Bang Nguyễn Quỳnh Anh
22520061	Nguyễn Thị Lan Anh
22520185	Nguyễn Thị Trâm Đan
22520066	Nguyễn Trần Bảo Anh

1. Từ trang web của MegaCorp One, hãy mô tả một chút về lĩnh vực hoạt động của công ty?

MegaCorp One hoạt động trong lĩnh vực công nghệ nano, với trọng tâm là nghiên cứu và phát triển các ứng dụng của công nghệ nano trong nhiều lĩnh vực khác nhau, bao gồm:

- Y tế: MegaCorp One đang phát triển các ứng dụng nano trong chẩn đoán và điều trị bệnh tật, chẳng hạn như các loại thuốc nano, các thiết bị y tế nano và các phương pháp điều trị mới dựa trên nano.
- Năng lượng: MegaCorp One đang phát triển các ứng dụng nano trong lĩnh vực năng lượng, chẳng hạn như các vật liệu nano hiệu quả hơn để lưu trữ năng lượng, các tế bào nhiên liệu nano và các phương pháp sản xuất năng lượng mới dựa trên nano.
- Môi trường: MegaCorp One đang phát triển các ứng dụng nano trong lĩnh vực môi trường, chẳng hạn như các vật liệu nano để lọc chất ô nhiễm, các phương pháp xử lý chất thải mới dựa trên nano và các vật liệu nano để tái chế.
- Sản xuất: MegaCorp One đang phát triển các ứng dụng nano trong lĩnh vực sản xuất, chẳng hạn như các vật liệu nano để sản xuất các sản phẩm mới, các quy trình sản xuất mới dựa trên nano và các phương pháp sản xuất bền vững hơn dựa trên nano.

Ngoài ra, MegaCorp One còn cung cấp các dịch vụ liên quan đến công nghệ nano, chẳng hạn như tư vấn, đào tạo và chuyển giao công nghệ.

2. Hãy liệt kê những thành viên đang làm việc cho MegaCorp One và một vài thông tin về những thành viên đó (địa chỉ email, chức vụ, tài khoản mạng xã hội)?

Những thành viên và thông tin thành viên đang làm việc cho MegaCorp One:

1. Joe Sheer

- Chức vụ: Tổng Giám Đốc Điều Hành
- Email: joe@megacorpone.com

2. Tom Hudson

- Chức vụ: Thiết Kế Web
- Email: thudson@megacorpone.com

3. Tanya Rivera

- Chức vụ: Nhà Phát Triển Cao Cấp
- Email: trivera@megacorpone.com

4. Matt Smith

- Chức vụ: Giám Đốc Tiếp Thị
- Email: msmith@megacorpone.com

5. Mike Carlow

- Chức vụ: Phó Chủ tịch Phụ Trách Pháp Lý
- Email: mcarlow@megacorpone.com

6. Alan Grofield

- Chức vụ: Giám Đốc CNTT và An Ninh
- Email: agrofield@megacorpone.com

3. Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra được điều gì?

Khi có được địa chỉ Email của các thành viên thuộc tổ chức thì đều có chung đuôi mail (@megacorpone.com) là thuộc công ty megacorpone.

Đầu mail là tên của nhân viên. Trừ Tổng giám đốc điều hành joe@megacorpone.com

4. Sử dụng công cụ whois để xác định các name server của MegaCorp One.

Các Name server của Magacorp One là:

- Name Server: NS1.MEGACORPONE.COM
- Name Server: NS2.MEGACORPONE.COM
- Name Server: NS3.MEGACORPONE.COM

```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ whois megacorpone.com
Domain Name: MEGACORPONE.COM
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2023-12-22T21:06:28Z
Creation Date: 2013-01-22T23:01:00Z
Registry Expiry Date: 2025-01-22T23:01:00Z
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.MEGACORPONE.COM
Name Server: NS2.MEGACORPONE.COM
Name Server: NS3.MEGACORPONE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-24T07:29:38Z <<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

5. Sử dụng công cụ whois để tìm kiếm các thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn) có được không? Giải thích?

Sử dụng công cụ whois không thể tìm kiếm các thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn). Vì tên miền uit.edu.vn không đăng ký thông qua các tổ chức đăng ký tên miền (domain registrars).

Thông tin về người hoặc tổ chức đăng ký tên miền được lưu trữ trong cơ sở dữ liệu công khai tại “<http://www.vnnic.vn/en>”. Dịch vụ whois cho phép người dùng truy vấn và xem thông tin này.

```
[(kali㉿kali)-[~]]$ whois uit.edu.vn
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
```

6. Thu thập thông tin về tên miền uit.edu.vn và hãy cho biết các thông tin như:

- Ngày đăng ký tên miền
- Ngày hết hạn tên miền
- Chủ sở hữu tên miền
- Các name server của tên miền

VNNIC INTERNET RESOURCE WHOIS INFORMATION

This whois query was received from IP Address: 14.191.220.43

We recognize the resource in your query is: Domain Name

Type of domain name: ASCII Domain Name

Keyword in your query: uit.edu.vn

Domain information

Domain Name:	uit.edu.vn
Registrant Name:	Trường Đại học Công nghệ Thông tin
Registrar:	Công ty TNHH PA Việt Nam
Creation Date:	2006-10-02
Expiration Date:	2029-10-02
Status:	clientTransferProhibited
Nameserver:	ns1.pavietnam.vn ns2.pavietnam.vn nsbak.pavietnam.net
DNSSEC:	unsigned

- a. Ngày đăng ký tên miền: 02/10/2006
- b. Ngày hết hạn tên miền: 02/10/2029
- c. Chủ sở hữu tên miền: Trường Đại Học Công Nghệ Thông Tin
- d. Các name server của tên miền:
 - ns1.pavietnam.vn
 - ns2.pavietnam.vn
 - https://nsbak.pavietnam.net/

7. Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?

- Phó chủ tịch Pháp lý của MegaCorp One là Mike Carlow
- Địa chỉ Gmail: mcarlow@megacorpone.com

Name: Mike Carlow

Title: VP Of Legal

Email: mcarlow@megacorpone.com

8. Bạn có thể tìm kiếm thêm các nhân viên khác của MegaCorp One mà không được liệt kê trên trang web www.megacorpone.com?

Các nhân viên khác: Mike Carlow, Sam Hilker, Mutunga Muli, Vicuong Ha, Emac Oscp, ...

The screenshot shows a website interface for "MegaCorp One". On the left, there's a navigation bar with "Company Information", "Email Format" (which is selected), "Management", and "Technology Stack". Below this, a section titled "MegaCorp One Email Format" features a LinkedIn icon and a button that says "Get Verified Emails for 16 MegaCorp One Employees". A note below the button states "3 free lookups per month. No credit card required." A blue arrow points from this section to the right side of the screen.

MegaCorp One Email Formats and Examples

Email Format	Example	Percentage
[first]	jane@megacorpone.com	100.0%

Email Verification Tool

Instantly check any MegaCorp One email. Get free lookups per month.

Enter name or email Verify →

Top MegaCorp One Employees

- Mike Carlow**
VP of Legal Affairs at
MegaCorp One
Henderson, NV, US
[View](#)
- Sam Hilker**
Sales Associate at
MegaCorp One
Wilmington, NC, US
[View](#)
- Mutunga Muli**
Electrical Specialist at
MegaCorp One
Nairobi County, Kenya
[View](#)
- Vicuong Ha**
Manager at MegaCorp One
Vietnam
[View](#)
- Emac Oscp**
Senior Tester at MegaCorp One
Deadwood, SD, US
[View](#)
- Ga Rod**
Boss at MegaCorp One
Panama City Beach, FL, US
[View](#)

9. Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa)

- **site:** Chỉ tìm kiếm trên một tên miền cụ thể.

Ví dụ: site:uit.edu.vn

- **filetype:** Tìm kiếm các tệp có định dạng cụ thể.

Ví dụ: filetype:pdf

- **intitle:** Tìm kiếm các trang web có tiêu đề chứa từ khóa.

Ví dụ: intitle:"login"

- **inurl:** Tìm kiếm các trang web có URL chứa từ khóa.

Ví dụ: inurl:admin

- **Cache:** Tìm kiếm phiên bản lưu trữ của một trang web trên Google Cache.

Ví dụ: cache:uit.edu.vn

**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 bạn là không nên được công bố?
site:uit.edu.vn "phone" OR "contact" OR "email"**

https://sdh.uit.edu.vn/sites/default/files/201804/ds_giao_de_tai_dot_1_2018.pdf

site:uit.edu.vn "username" OR "password"

https://httt.uit.edu.vn/en_US/nghien-cuu-khoa-hoc/danh-sach-de-tai-nckh-sinh-vien/

site:uit.edu.vn "confidential" OR "internal" filetype:pdf

https://www.uit.edu.vn/sites/vi/files/uploads/images/202109/cong_khai_nam_hoc_2020-2021.pdf

11. Sử dụng Netcraft để xác định máy chủ ứng dụng (application server) đang chạy trên www.megacorpone.com

The screenshot shows a browser window with a Netcraft site report for the URL <http://www.megacorpone.com>. The report includes the following information:

Category	Value
IPv4 autonomous systems	AS16276
IPv6 address	Not Present
IPv6 autonomous systems	Not Present
Reverse DNS	www.megacorpone.com
Domain	megacorpone.com
Nameserver	ns1.megacorpone.com
Domain registrar	gandi.net
Nameserver organisation	whois.gandi.net
Organisation	MegaCorpOne, Rachel, 89001, United States
DNS admin	admin@megacorpone.com
Top Level Domain	Commercial entities (.com)
DNS Security Extensions	Enabled

At the bottom of the report, there is a section titled "IP delegation" which lists several IP addresses and their corresponding network ranges.

Máy chủ là: ns1.megacorpone.com

12. Thực hiện sử dụng module có thể giúp phân giải tên miền ở Hình 20 thành địa chỉ IP tương ứng.

Sử dụng module recon/domains-hosts/hackertarget để lấy IP

www.megacorpone.com

```
[*] 1 total (1 new) hosts found.
[recon-ng][default][hackertarget] > options set SOURCE www.megacorpone.com
SOURCE => www.megacorpone.com
[recon-ng][default][hackertarget] > run

_____
WWW.MEGACORPONE.COM

[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
_____
SUMMARY

[*] 1 total (1 new) hosts found.
[recon-ng][default][hackertarget] > █
```

Vpn.megacorpone.com

```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE vpn.megacorpone.com
SOURCE => vpn.megacorpone.com
[recon-ng][default][hackertarget] > run

_____
VPN.MEGACORPONE.COM

[*] Country: None
[*] Host: vpn.megacorpone.com
[*] Ip_Address: 167.114.21.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
_____
SUMMARY

[*] 1 total (1 new) hosts found.
[recon-ng][default][hackertarget] > █
```

Siem.megacorpone.com

```
[recon-ng][default][hackertarget] > options set SOURCE siem.megacorpone.com  
SOURCE => siem.megacorpone.com  
[recon-ng][default][hackertarget] > run
```

SIEM.MEGACORPONE.COM

```
[*] Country: None  
[*] Host: siem.megacorpone.com  
[*] Ip_Address: 167.114.21.71  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]
```

SUMMARY

```
[*] 1 total (1 new) hosts found.  
[recon-ng][default][hackertarget] > █
```

Www2.megacorpone.com

```
[recon-ng][default][hackertarget] > options set SOURCE www2.megacorpone.com  
SOURCE => www2.megacorpone.com  
[recon-ng][default][hackertarget] > run
```

WWW2.MEGACORPONE.COM

```
[*] Country: None  
[*] Host: www2.megacorpone.com  
[*] Ip_Address: 149.56.244.87  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]
```

SUMMARY

```
[*] 1 total (1 new) hosts found.  
[recon-ng][default][hackertarget] > █
```

Intranet.megacorpone.com

```
[recon-ng][default][hackertarget] > options set SOURCE intranet.megacorpone.com
SOURCE => intranet.megacorpone.com
[recon-ng][default][hackertarget] > run

_____
INTRANET.MEGACORPONE.COM

[*] Country: None
[*] Host: intranet.megacorpone.com
[*] Ip_Address: 167.114.21.67
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
_____

SUMMARY
_____
[*] 1 total (1 new) hosts found.
[recon-ng][default][hackertarget] > █
```

Support.megacorpone.com

```
[*] 1 total (1 new) hosts found.
[recon-ng][default][hackertarget] > options set SOURCE support.megacorpone.com
SOURCE => support.megacorpone.com
[recon-ng][default][hackertarget] > run

_____
SUPPORT.MEGACORPONE.COM

[*] Country: None
[*] Host: support.megacorpone.com
[*] Ip_Address: 167.114.21.74
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
_____

SUMMARY
_____
[*] 1 total (1 new) hosts found.
[recon-ng][default][hackertarget] > █
```

13. Sử dụng một số module khác có trong recon-ng để thu thập thông tin về UIT nhiều nhất có thể.

Sử dụng module recon/domains-hosts/hackertarget

kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

kali@kali: ~

```
[*] Invalid module path.
[*] Marketplace install recon/domains-hosts/namechk
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[*] Modules load recon/domains-hosts/hackertarget
[*] Options set SOURCE uit.edu.vn
SOURCE => uit.edu.vn
[recon-ng][default][hackertarget] > run

UIT.EDU.VN
[*] Country: None
[*] Host: acm.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: auth.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: band1.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: banglcs.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: cd.uit.edu.vn
[*] Ip_Address: 45.122.249.78
```

kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

kali@kali: ~

```
[*] Country: None
[*] Host: cd.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: chungthuc.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: cnpm.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: cnsn.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: competitions.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: congdoan.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

```
[*] Country: None
[*] Host: courses.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: cs.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: service.aiclub.cs.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www.service.aiclub.cs.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: tutorials.aiclub.cs.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www.tutorials.aiclub.cs.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
```

```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[*] longilude:None
    Notes: None
    Region: None
[*] -> host:None
    Host: console-cloud.vlab.uit.edu.vn
    Id_Address: 45.122.249.74
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
[*] -> host:None
    Country: None
    Host: vpn.uit.edu.vn
    Id_Address: 42.116.6.42
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
[*] -> host:None
    Country: None
    Host: www.uit.edu.vn
    Id_Address: 118.69.123.140
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
[*] -> host:None
    Country: None
    Host: versashell.uit.edu.vn
    Id_Address: 118.69.123.140
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
[*] -> host:None
    Country: None
    Host: www.uit.edu.vn
    Id_Address: 45.122.249.74
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
SUMMARY
[*] 87 total (87 new) hosts found.
[recon-ng][default]> back
[recon-ng][default]> show hosts
+-----+
| rowid | host | ip_address | region | country |
+-----+
| 1     | admin.megacorpone.com | 45.122.249.78 | | |
| 2     | www.megacorpone.com | netcraft | | |
| 3     | support.megacorpone.com | netcraft | | |
| 4     | intranet.megacorpone.com | netcraft | | |
| 5     | acm.uit.edu.vn | netcraft | | |
| 6     | auth.uit.edu.vn | hackertarget | | |
| 7     | bandl.uit.edu.vn | hackertarget | | |
| 8     | banglcs.uit.edu.vn | hackertarget | | |
| 9     | cd.uit.edu.vn | hackertarget | | |
| 10    | chungthuc.uit.edu.vn | hackertarget | | |
| 11    | cnpm.uit.edu.vn | hackertarget | | |
| 12    | cnsc.uit.edu.vn | hackertarget | | |
| 13    | competitions.uit.edu.vn | 45.122.249.78 | | |
| 14    | congdoan.uit.edu.vn | hackertarget | | |
| 15    | courses.uit.edu.vn | hackertarget | | |
| 16    | cs.uit.edu.vn | hackertarget | | |
| 17    | service.aiclub.cs.uit.edu.vn | 118.69.123.140 | | |
+-----+
```

```
Rain showers
Sunday
5:31 PM
10/25/2024
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[*] -> host:None
    Host: console-cloud.vlab.uit.edu.vn
    Id_Address: 45.122.249.74
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
[*] -> host:None
    Country: None
    Host: vpn.uit.edu.vn
    Id_Address: 42.116.6.42
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
[*] -> host:None
    Country: None
    Host: www.uit.edu.vn
    Id_Address: 118.69.123.140
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
[*] -> host:None
    Country: None
    Host: versashell.uit.edu.vn
    Id_Address: 118.69.123.140
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
[*] -> host:None
    Country: None
    Host: www.uit.edu.vn
    Id_Address: 45.122.249.74
    Latitude: None
    Longitude: None
    Notes: None
    Region: None
SUMMARY
[*] 87 total (87 new) hosts found.
[recon-ng][default]> back
[recon-ng][default]> show hosts
+-----+
| rowid | host | ip_address | region | country |
+-----+
| 1     | admin.megacorpone.com | 45.122.249.78 | | |
| 2     | www.megacorpone.com | netcraft | | |
| 3     | support.megacorpone.com | netcraft | | |
| 4     | intranet.megacorpone.com | netcraft | | |
| 5     | acm.uit.edu.vn | netcraft | | |
| 6     | auth.uit.edu.vn | hackertarget | | |
| 7     | bandl.uit.edu.vn | hackertarget | | |
| 8     | banglcs.uit.edu.vn | hackertarget | | |
| 9     | cd.uit.edu.vn | hackertarget | | |
| 10    | chungthuc.uit.edu.vn | hackertarget | | |
| 11    | cnpm.uit.edu.vn | hackertarget | | |
| 12    | cnsc.uit.edu.vn | hackertarget | | |
| 13    | competitions.uit.edu.vn | 45.122.249.78 | | |
| 14    | congdoan.uit.edu.vn | hackertarget | | |
| 15    | courses.uit.edu.vn | hackertarget | | |
| 16    | cs.uit.edu.vn | hackertarget | | |
| 17    | service.aiclub.cs.uit.edu.vn | 118.69.123.140 | | |
+-----+
```

86°F
Partly sunny

5:34 PM
10/25/2024

```

kali@kali: ~
File Actions Edit View Help
| 70 | student.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 71 | tchc.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 72 | techcovid.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 73 | gw.techcovid.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 74 | hcmcovidsafe_techcovid.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 75 | hcmcovidsafe-dev_techcovid.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 76 | hcmcovidsafe-dev_techcovid.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 77 | www.hcmcovidsafe-dev_ge_techcovid.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 78 | www.hcmcovidsafe-dev_techcovid.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 79 | hcmcovidsafe-gw_techcovid.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 80 | www.hcmcovidsafe_techcovid.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 81 | thuvien.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 82 | tracngheim.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 83 | ttpdbcl.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 84 | tuyensinh.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 85 | vinhdanh.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 86 | vlab.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 87 | 519b0137d6144dbeda18e0d3a8da0-s-80.vlab.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 88 | console-cloud.vlab.uit.edu.vn | hackettarget | | 45.122.249.78 | | |
| 89 | vpn.uit.edu.vn | hackettarget | | 42.116.6.42 | | |
| 90 | www.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
| 91 | zeroshell.uit.edu.vn | hackettarget | | 118.69.123.140 | | |
+-----+
[*] 91 rows returned
[recon-ng][defaultValue] > 

```

Sử dụng module recon/profiles-profiles/profiler

```

SUMMARY
[*] 4 total (4 new) profiles found.
[recon-ng][defaultValue] > show profiles
+-----+
| rowid | username | resource | url | category | notes | module |
| 1 | uit.edu.vn | chatango.com | https://uit.edu.vn.chatango.com | social | | profiler |
| 2 | uit.edu.vn | MANYVIDS | https://www.manyvids.com/results.php?keywords=uit.edu.vn | xx NSPxx | | profiler |
| 3 | uit.edu.vn | Mastodon-mew.social | https://mew.social/@uit.edu.vn | social | | profiler |
| 4 | uit.edu.vn | tumblr | https://uit.edu.vn.tumblr.com | images | | profiler |
+-----+
[*] 4 rows returned
[recon-ng][defaultValue] > 

```

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

15. Thực hiện tìm kiếm các lệnh khác trên Shodan mà có thể tiết lộ thêm nhiều thông tin thú vị về một đối tượng bất kỳ.

Apache: trả về các máy chủ chạy phần mềm apache

apache - Shodan Search

shodan.io/search?query=apache

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing | apache | Search | Login

TOTAL RESULTS
18,405,600

TOP COUNTRIES

Country	Count
United States	5,216,798
Germany	1,841,061
Japan	1,664,906
China	1,354,660
France	803,606
More...	

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

Native Power Technology Co.,Ltd. [View Report](#) [Browse Images](#) [View on Map](#) [Advanced Search](#)

192.185.57.168
Issued By: R10
Server: Apache
P3P: CP="NOT ADM DEV PSAI COM NAV OUR OTRo STP IND DEM"
Permissions-Policy: interest-cohort=()
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-...

SSL Certificate
Let's Encrypt
Supported SSL
Versions:
TLSv1.2, TLSv1.3

Site inexistant [View Report](#) [Browse Images](#) [View on Map](#) [Advanced Search](#)

95.128.73.237
Issued To: nativepowertechnology.com
HTTP/1.1 200 OK

2024-10-25T13:45:04.319567

2024-10-25T13:45:00.674453

Cisco.ios: trả về các thiết bị chạy hệ điều hành IOS của Cisco

cisco-ios - Shodan Search

shodan.io/search?query=cisco-ios

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing | cisco-ios | Search | Login

TOTAL RESULTS
99,619

TOP COUNTRIES

Country	Count
United States	13,695
India	7,468
Mexico	3,944
Brazil	3,032
France	2,885
More...	

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

102.217.48.19 [View Report](#) [Browse Images](#) [View on Map](#) [Advanced Search](#)

DFA Zimbabwe (Private) Limited
Zimbabwe, Bulawayo
SNMP:
Uptime: 601901541
Description: Cisco IOS XR Software (Cisco ASR9K Series), Version 6.9.2[Default]
Copyright (c) 2023 by Cisco Systems, Inc.
Service: 78
Versions:
1
3
Name: HREBN-ASR9001-01.dfafrica.co.zw
Engine Boots: 13
Engineid Data: 00000000030010f31132ec26
Ente...

195.113.187.169 [View Report](#) [Browse Images](#) [View on Map](#) [Advanced Search](#)

Významný ustanovitelský techniky
HTTP/1.1 401 Unauthorized
Date: Fri, 25 Oct 2024 13:28:20 GMT

2024-10-25T13:41:09.414728

2024-10-25T13:39:41.375674

Port:25: Lọc kết quả theo số cổng cụ thể của dịch vụ hoặc tìm các cổng cụ thể đang mở

TOTAL RESULTS
4,818,341

TOP COUNTRIES

Country	Count
United States	1,582,186
Germany	546,852
Japan	386,488
France	308,472
China	259,686
More...	

45.223.191.131

Incapsula Inc
Brazil, São Paulo
cdn

HTTP/1.1 400 Bad Request
Content-Type: text/html
Cache-Control: no-cache, no-store
Connection: close
Content-Length: 705
X-Info: 15-295378139-0 0NNN RT(1729863866012 1003) q(-1 -1 -1 -1) r(0 -1) b1
html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name...

154.56.135.218

dns135218.phdns18.es
SOLUCIONES WEB ON LINE S.L.
Spain, Madrid
starttls

SSL Certificate
Issued By: R11
- Common Name: 220 dns135218.phdns18.es ESMTP
- Organization: Let's Encrypt
250-dns135218.phdns18.es
250-AUTH=LOGIN CRAM-MDS PLAIN
250-LOGIN CRAM-MDS PLAIN
250-STARTTLS
250-PIPELINING

City:Hanoi: Lọc kết quả theo mã quốc gia cụ thể gồm hai chữ số hoặc tìm thiết bị ở một quốc gia cụ thể.

TOTAL RESULTS
1,165,802

TOP PORTS

Port	Count
80	112,321
443	83,456
22	76,474
2000	39,875
554	29,000
More...	

TOP ORGANIZATIONS

Organization	Count
Viettel Group	293,515
FPT Telecom Company	160,432
Vietnam Posts and Tele...	123,595
African Network Informat...	63,785

1.53.67.89

FPT Telecom Company
Viet Nam, Hanoi

MikroTik Winbox:
list:
adtool.jg: 7.15.3
container.jg: 7.15.3
dhcp.jg: 7.15.3
hotspot.jg: 7.15.3
icons.png: 7.15.3
icons24.png:
icons32.png:
ipv6.jg: 7.15.3
ppp.jg: 7.15.3
rot eros.jg: 7.15.3
secure.jg: 7.15.3
ups.jg: 7.15.3
wave2.jpg: 7.15.3...

58.186.173.9

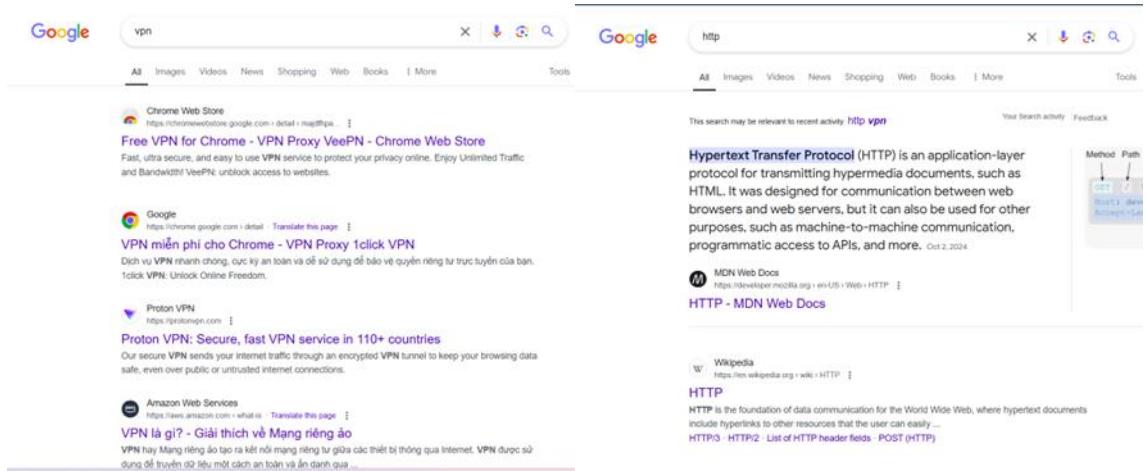
FPT Telecom Company
RTSP/1.0 401 Unauthorized

16. So sánh kết quả tìm kiếm trên Shodan so với các search engine khác như Google, Bing...
Kết quả tìm kiếm trên Shodan:



- http: Tìm kiếm các thiết bị có dịch vụ web đang chạy trên cổng HTTP (cổng 80).
- vpn: Tìm kiếm các máy chủ đang chạy dịch vụ VPN

Kết quả tìm kiếm trên search engine khác (Google):



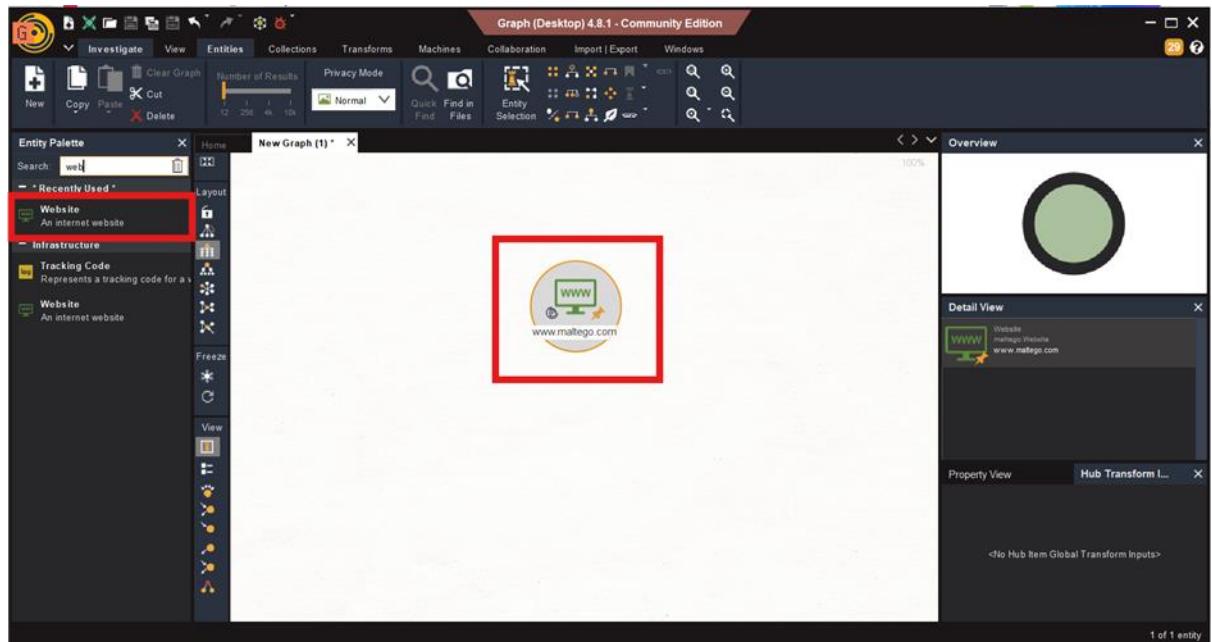
So sánh:

- **Shodan** là một công cụ tìm kiếm các thiết bị và dịch vụ kết nối với internet, bao gồm máy chủ, webcam, router, hệ thống điều khiển công nghiệp (ICS), IoT, v.v. Shodan không tìm kiếm nội dung web mà tập trung vào các thiết bị kết nối và các dịch vụ đang chạy trên các thiết bị đó.
- **Google** chủ yếu tìm kiếm nội dung trên các trang web, với mục tiêu cung cấp thông tin liên quan đến truy vấn của người dùng dựa trên các trang web và nội dung văn bản, hình ảnh, và video.

17. Sử dụng công cụ theHarvester để lấy tìm kiếm các địa chỉ email của UIT
18. Sử dụng với nguồn tìm kiếm khác (-b). Theo bạn, kết quả của nguồn nào tốt hơn?

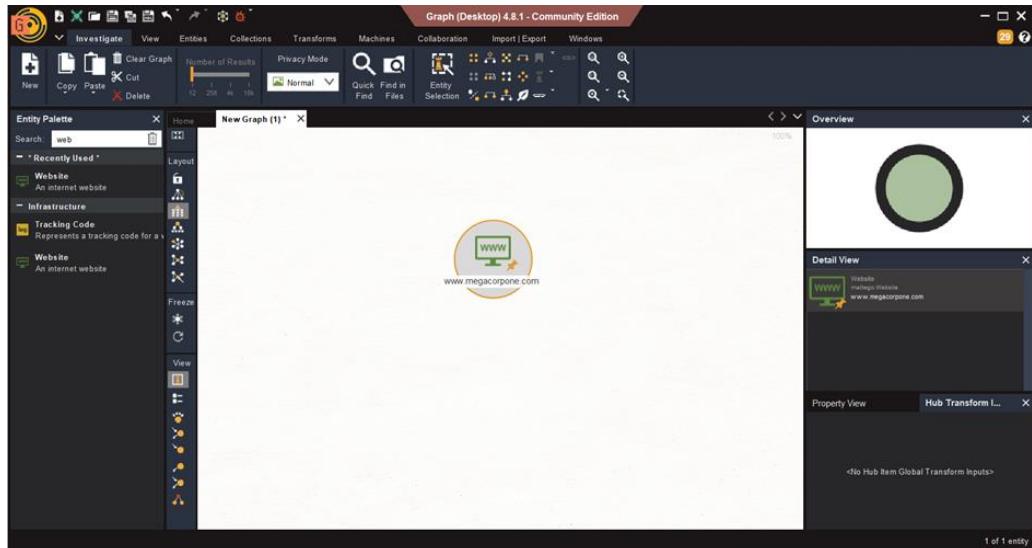
19.Thực hiện tìm kiếm các địa chỉ Email của MegaCorp One sử dụng Maltego

Bước 1: Bên trái, kiểm đến mục **Infrastructure**, giữ Website và kéo vào chỗ trống ở giữa.



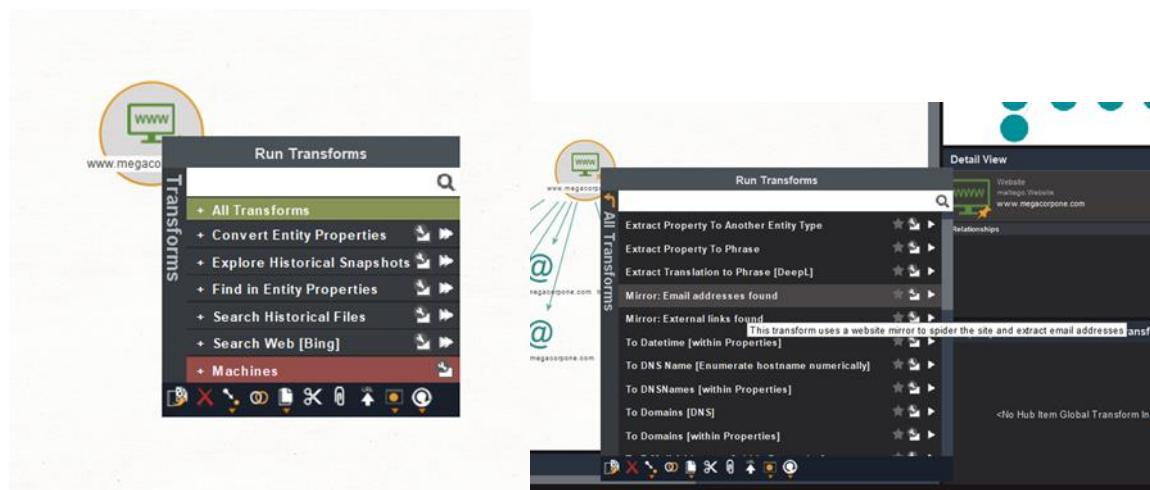
Bước 2: Thực thể website được xuất hiện, double click vào domain mặc định

(www.maltego.com) và sửa thành www.megacorpone.com

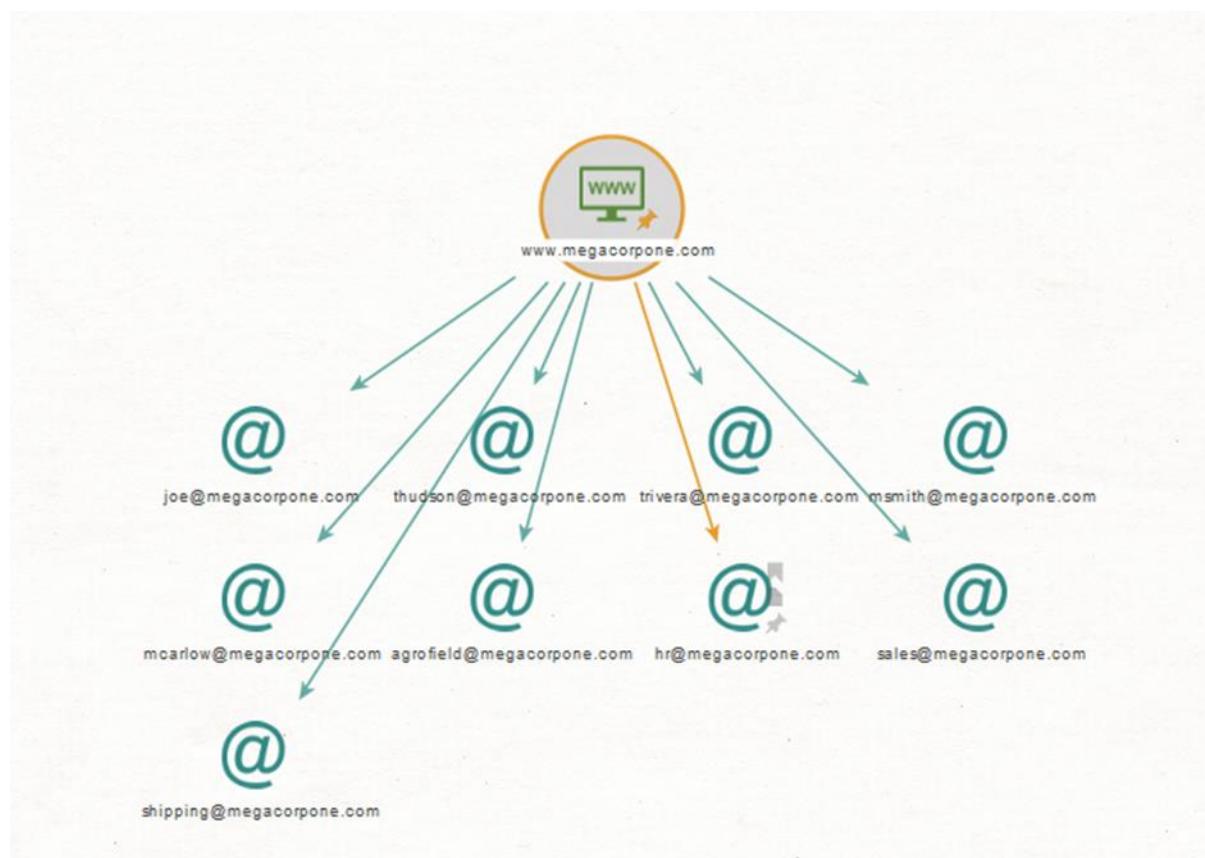


Bước 3: Chuột phải vào thực thể này vào chọn All Transforms.

Danh sách các Transforms xuất hiện, chọn Mirror: Email addresses found



Kết quả: Hiển thị các địa chỉ Email mà MegaCorp One sử dụng

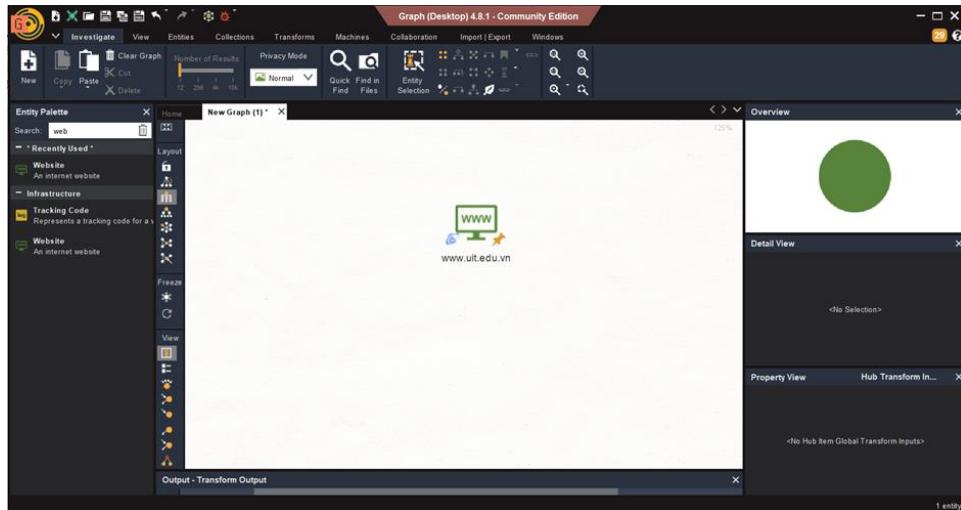


20. Sử dụng công cụ Maltego cho UIT (tên miền: uit.edu.vn) và trả lời các câu hỏi sau:

a. Các bản ghi DNS.

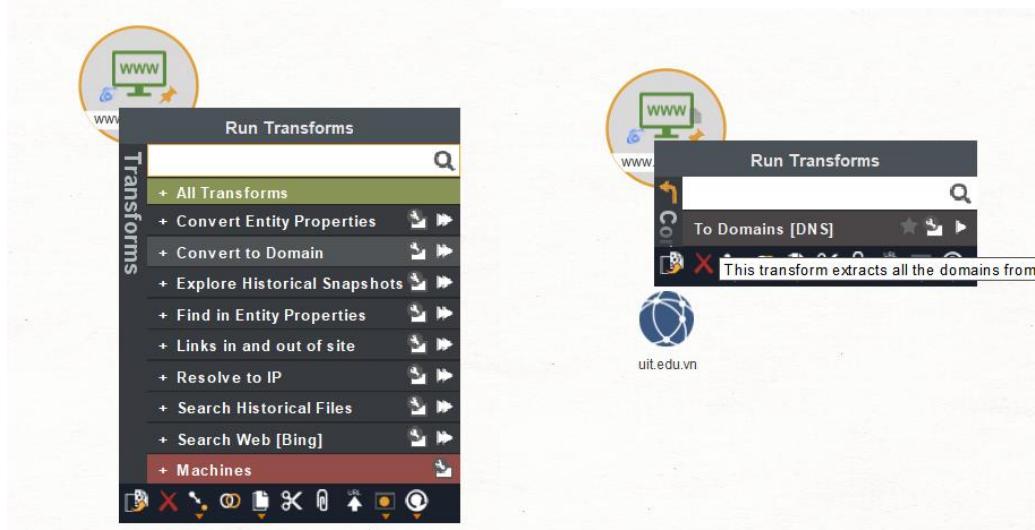
b. Các website và địa chỉ IP tương ứng.

Thực hiện tương tự bước 1 và 2 của câu 19, ta có:

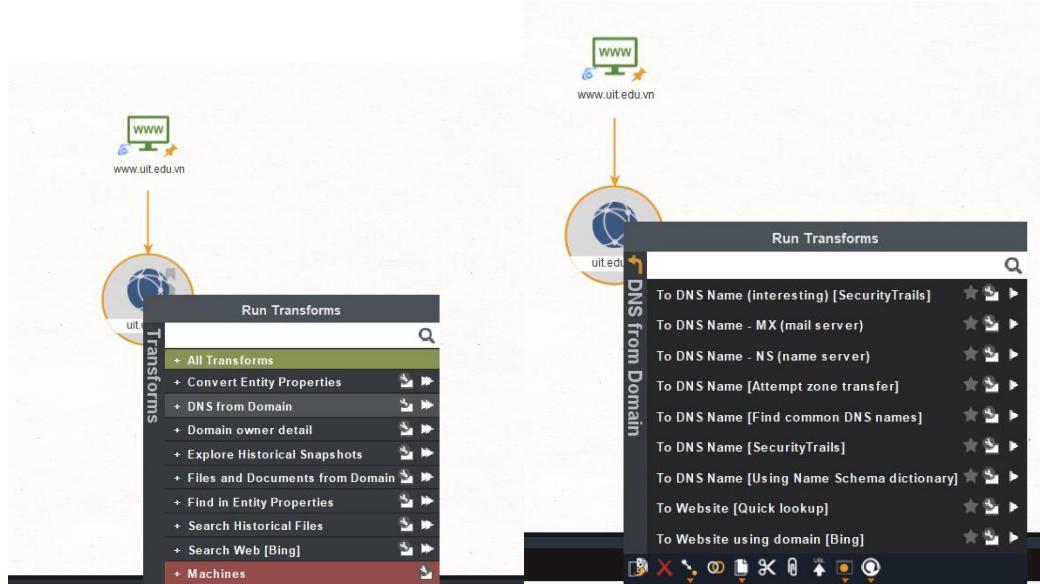


a. Các bản ghi DNS.

Bước 1: Chọn Convert to Domain -> To Domain [DNS]



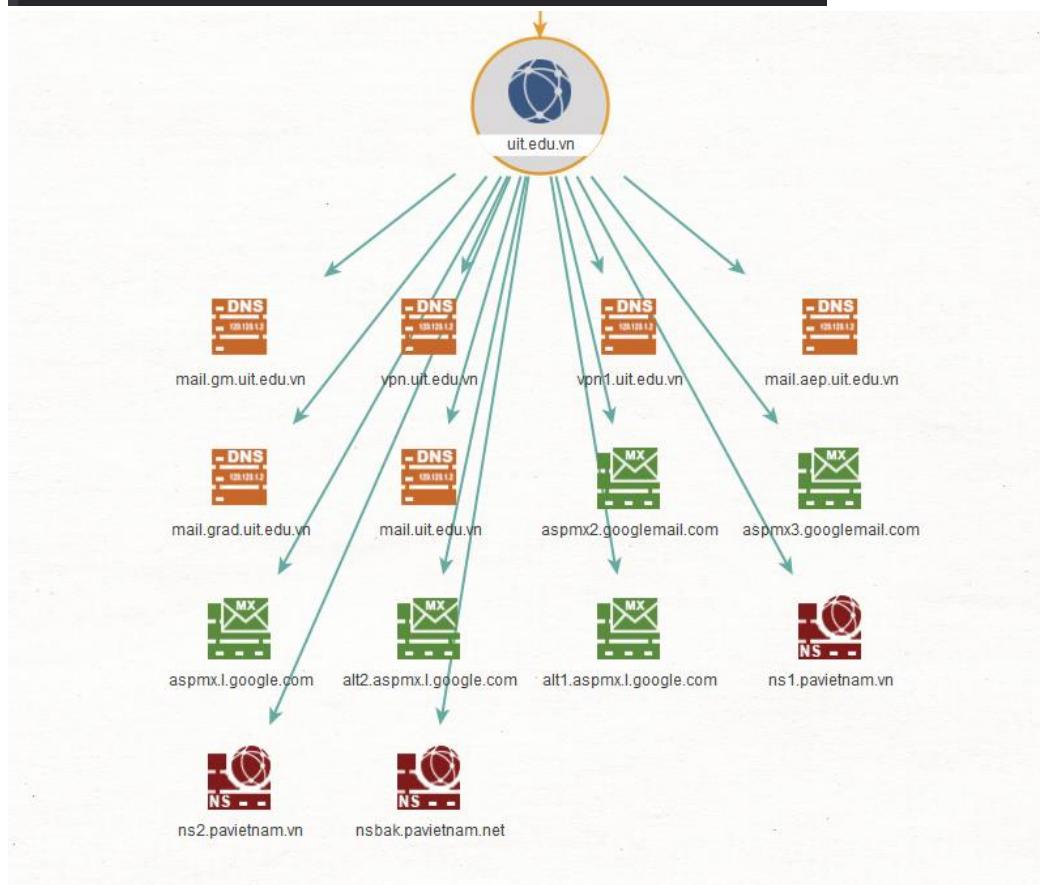
Bước 2: Chọn DNS from Domain -> Chọn lần lượt các bản ghi DNS trong danh sách



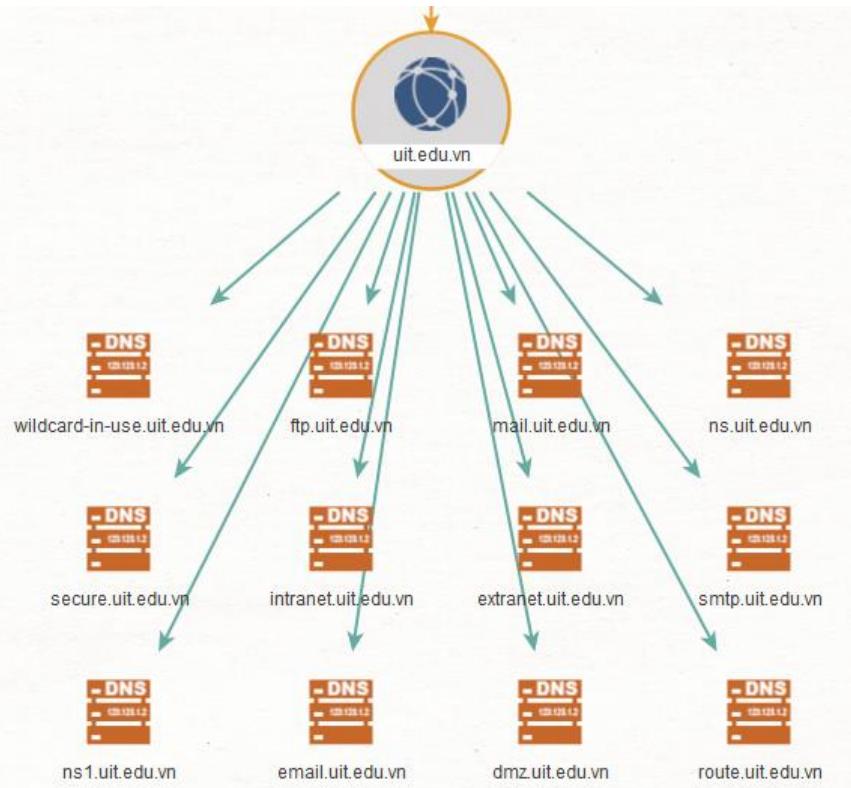
Kết quả:

Chọn 3 bản ghi DNS sau:

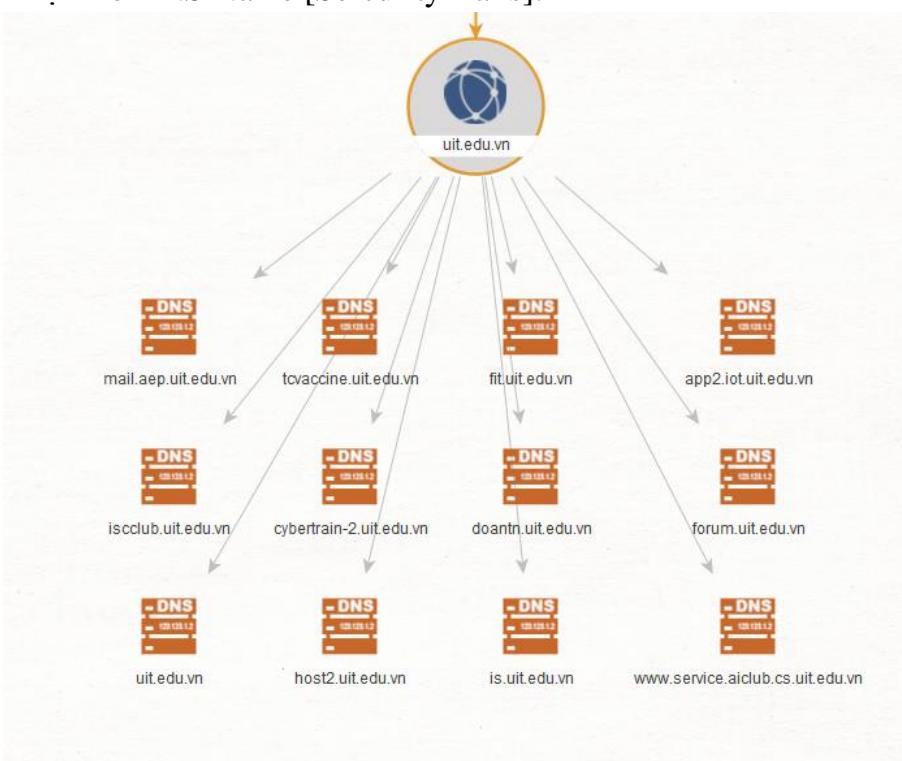
- | | |
|---|-------|
| To DNS Name (interesting) [SecurityTrails] | ★ 🔍 ► |
| To DNS Name - MX (mail server) | ★ 🔍 ► |
| To DNS Name - NS (name server) | ★ 🔍 ► |



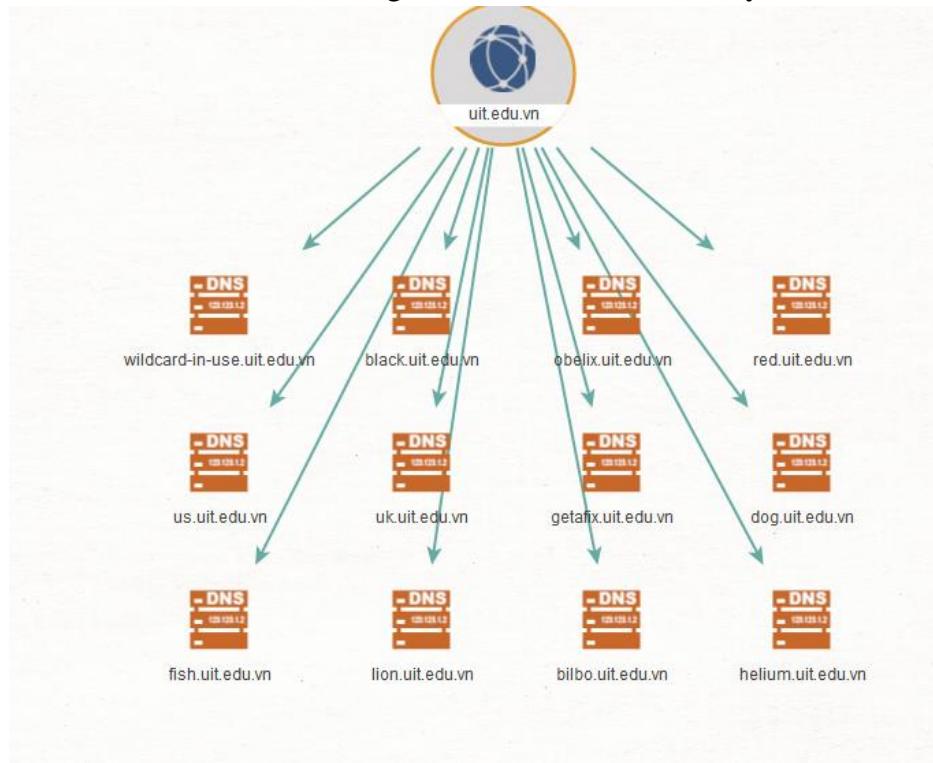
Chọn To DNS Name [Find common DNS names]:



Chọn To DNS Name [Security Trails]:

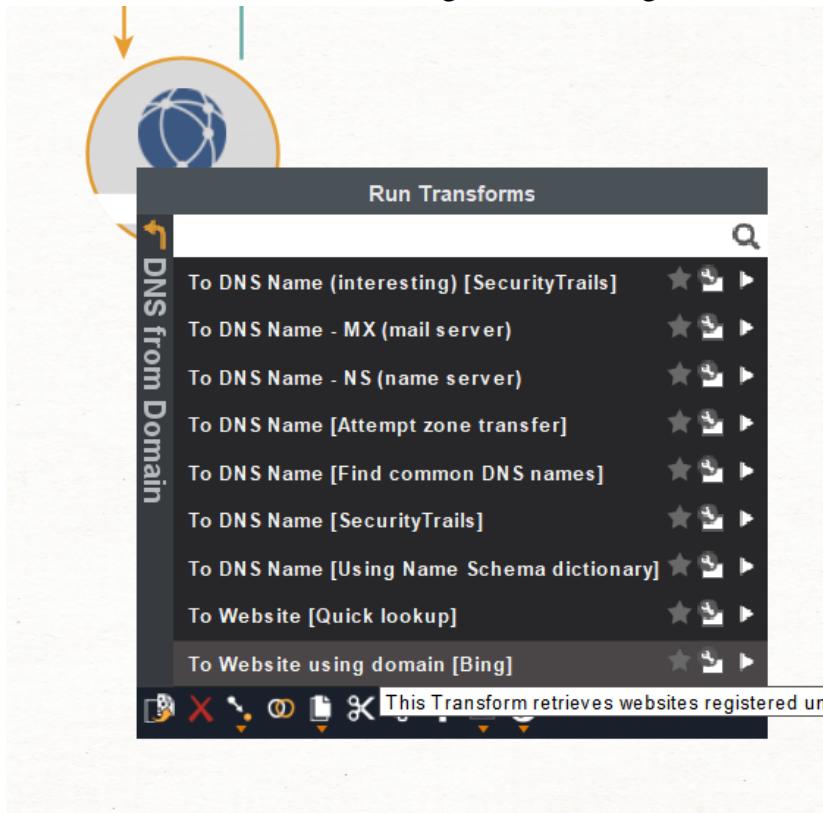


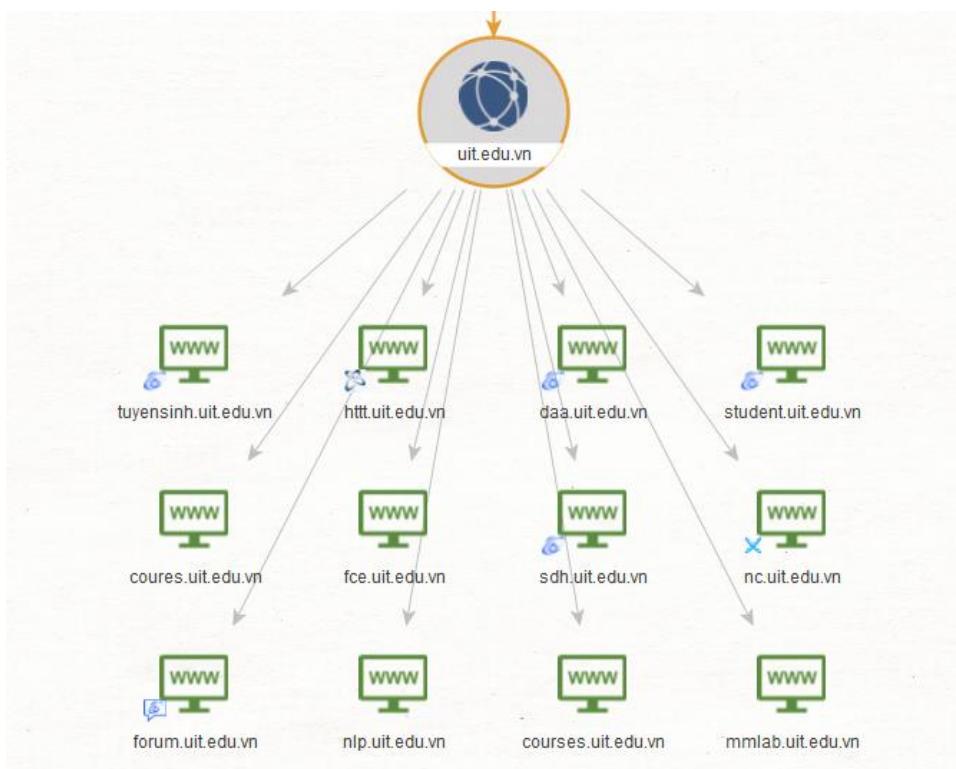
Chọn To DNS Name [Using Name Schema dictionary]:



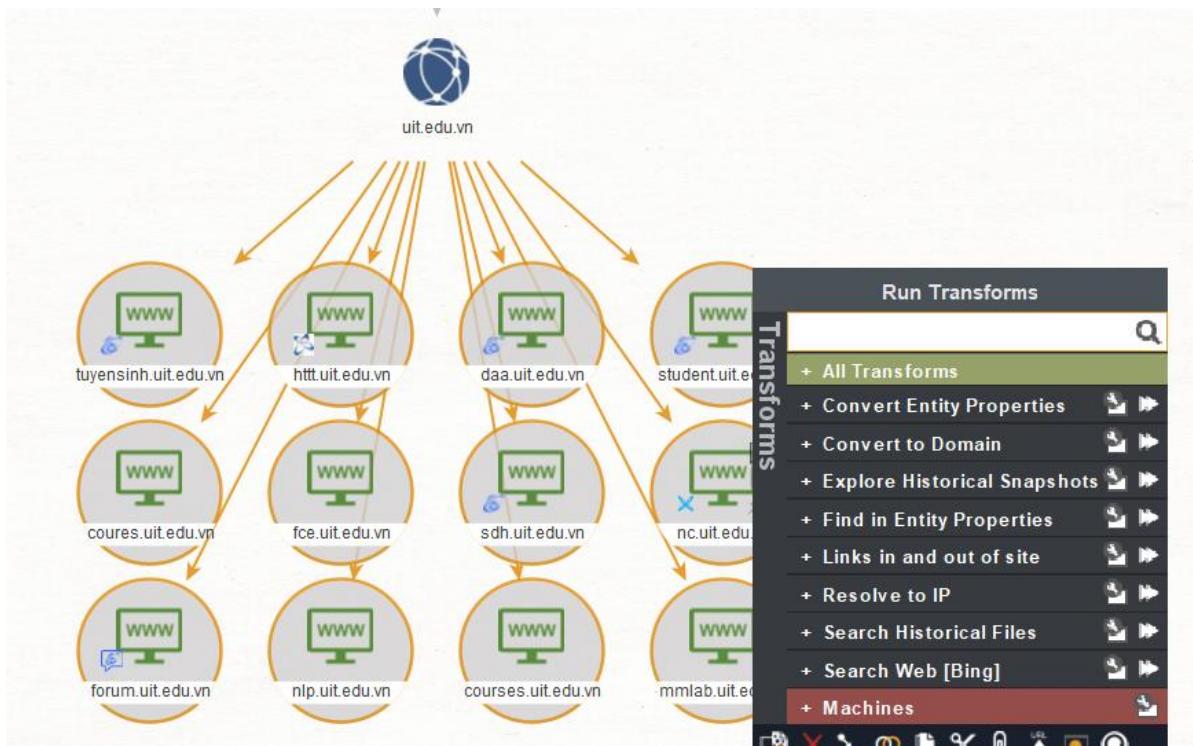
b. Các website và địa chỉ IP tương ứng

Bước 1: Chọn To Website using domain [Bing]

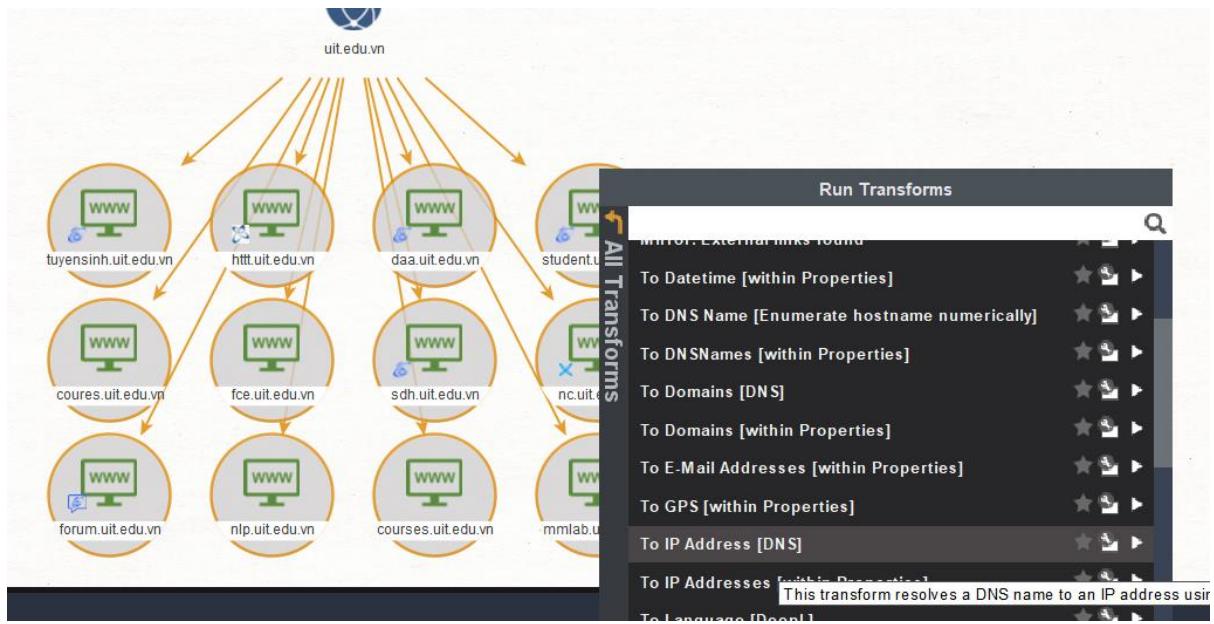




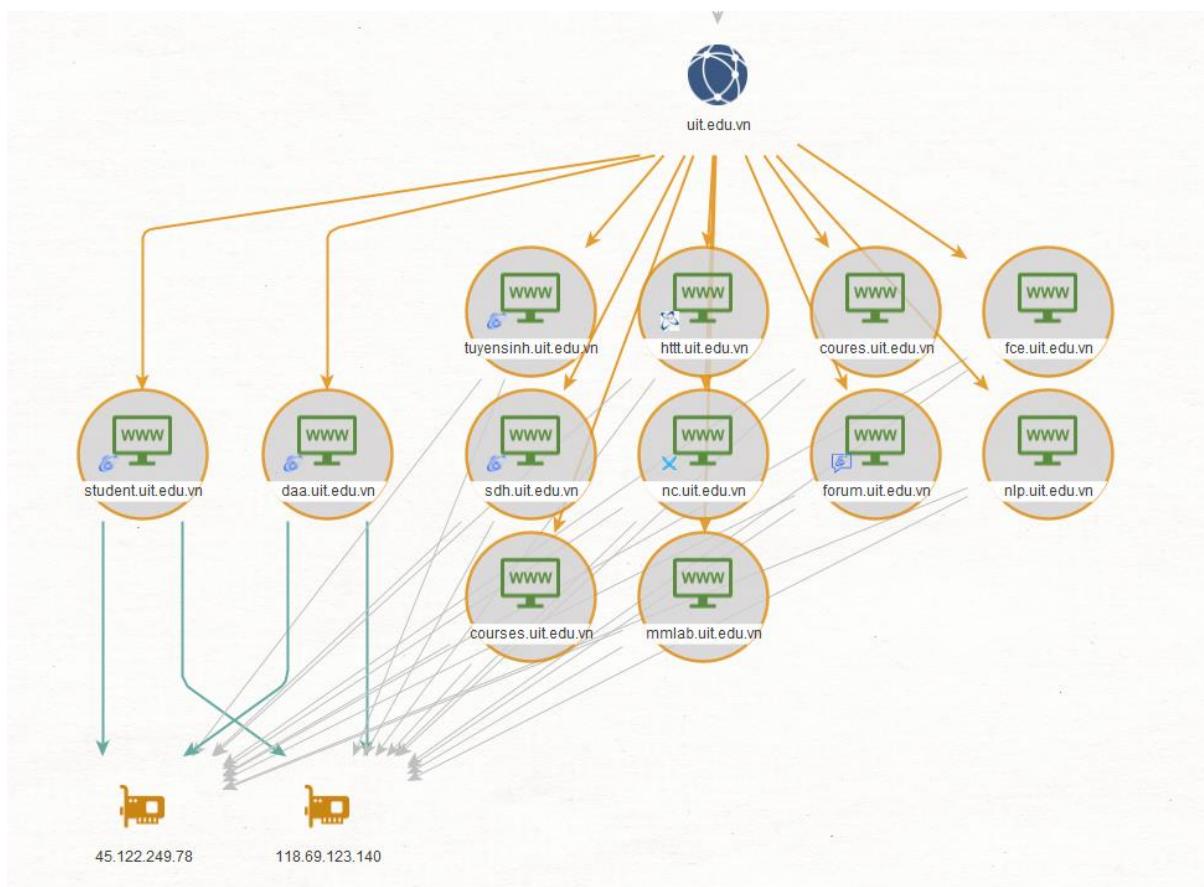
Bước 2: Chọn tất cả các đối tượng muốn xem địa chỉ IP, chọn All Transforms



Bước 3: Chọn To IP Address [DNS]



Kết quả:



Một số bản ghi DNS phổ biến nhất bao gồm:

- **NS** – Bản ghi Nameserver chứa tên của máy chủ có thẩm quyền (authoritative server) lưu trữ các bản ghi DNS cho một tên miền nào đó.

- **A** – Còn được gọi là bản ghi host, dùng để phân giải Host ra một địa chỉ 32-bit IPv4. Dùng để trỏ tên website như www.domain.com đến một Server Hosting website đó.
- **MX** – Bản ghi Mail Exchange chứa tên của các máy chủ có nhiệm vụ xử lý email cho tên miền. Một tên miền có thể chứa nhiều bản ghi MX
- **PTR** – Bản ghi Pointer được sử dụng trong reverse lookup zones và được sử dụng để tìm kiếm các hostname tương ứng với địa chỉ IP muốn tìm kiếm.
- **CNAME** – Bản ghi Canonical Name được sử dụng để tạo các bí danh (alias) cho các bản ghi host,
- **TXT** – Các bản ghi Text có thể chứa các dữ liệu bất kỳ và có thể được sử dụng cho các mục đích khác nhau, chẳng hạn như chứng nhận quyền sở hữu tên miền

a. Ngoài các bản ghi kể trên, hãy liệt kê các bản ghi khác của DNS.

- 1. AAAA (Quad-A Record):** Tương tự như bản ghi A, nhưng dùng để phân giải tên miền thành địa chỉ IP IPv6 (128-bit).
- 2. SOA (Start of Authority Record):** Bản ghi này chứa thông tin về máy chủ DNS chính chịu trách nhiệm cho tên miền, cùng với các thông tin về quản trị tên miền, bao gồm email của người quản trị, số serial của bản ghi, và các giá trị TTL (Time to Live) liên quan đến việc làm mới (refresh) và truy vấn lại.
- 3. SRV (Service Record):** Bản ghi này được sử dụng để xác định máy chủ cung cấp dịch vụ cụ thể (ví dụ như dịch vụ VoIP, XMPP, hoặc SIP) cho một tên miền.
- 4. CAA (Certification Authority Authorization):** Cho phép quản trị viên tên miền chỉ định các nhà cung cấp chứng chỉ số (CA) được phép phát hành chứng chỉ SSL/TLS cho tên miền đó.
- 5. NAPTR (Naming Authority Pointer Record):** Bản ghi NAPTR thường được dùng trong các dịch vụ chuyển hướng như SIP và ENUM, để chỉ định cách phân giải các địa chỉ URI hoặc tìm các dịch vụ liên quan đến giao thức nào đó.
- 6. HINFO (Host Information Record):** Bản ghi này chứa thông tin mô tả hệ điều hành (OS) và phần cứng của máy chủ. Tuy nhiên, hiện nay nó ít được sử dụng vì có thể tiềm ẩn rủi ro bảo mật.

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

Bản ghi TXT:

```
nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~$ dig txt uit.edu.vn

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> txt uit.edu.vn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 32752
;; flags: qr rd ad; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;uit.edu.vn.           IN      TXT

;; ANSWER SECTION:
uit.edu.vn.          0       IN      TXT      "_ukan9w1l3iica61scp6fwumq5v6dopw"
uit.edu.vn.          0       IN      TXT      "sqm6y27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn.          0       IN      TXT      "k6t321pqvf9jryb0z4n5scftqph6t781"
uit.edu.vn.          0       IN      TXT      "google-site-verification=wjArKGa37oHK083XqT2C91tPny8NLttGS0aU5pJjKiY"
uit.edu.vn.          0       IN      TXT      "svp60rjlwr6s19rn9t013cfwm3xmqx7h"
uit.edu.vn.          0       IN      TXT      "v=spf1 include:_spf.google.com ~all"
uit.edu.vn.          0       IN      TXT      "google-site-verification=z9wIF5gp5-YbdAQsttR2KmyHCPy3FN6Qk0GOBUWIrwc"
uit.edu.vn.          0       IN      TXT      "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"

;; Query time: 19 msec
;; SERVER: 172.25.128.1#53(172.25.128.1) (UDP)
;; WHEN: Fri Oct 25 18:28:29 +07 2024
;; MSG SIZE rcvd: 484

nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~$ |
```



```
nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~$ host -t txt uit.edu.vn
uit.edu.vn descriptive text "_ukan9w1l3iica61scp6fwumq5v6dopw"
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn descriptive text "k6t321pqvf9jryb0z4n5scftqph6t781"
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C91tPny8NLttGS0aU5pJjKiY"
uit.edu.vn descriptive text "svp60rjlwr6s19rn9t013cfwm3xmqx7h"
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"
uit.edu.vn descriptive text "google-site-verification=z9wIF5gp5-YbdAQsttR2KmyHCPy3FN6Qk0GOBUWIrwc"
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"
nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~$ |
```

Bản ghi MX:

```
nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~$ dig mx uit.edu.vn

; <>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> mx uit.edu.vn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 50916
;; flags: qr rd ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;uit.edu.vn.           IN      MX

;; ANSWER SECTION:
uit.edu.vn.          0       IN      MX      40 aspmx2.googlemail.com.
uit.edu.vn.          0       IN      MX      20 alt2.aspmx.l.google.com.
uit.edu.vn.          0       IN      MX      40 aspmx3.googlemail.com.
uit.edu.vn.          0       IN      MX      20 alt1.aspmx.l.google.com.
uit.edu.vn.          0       IN      MX      10 aspmx.l.google.com.

;; Query time: 30 msec
;; SERVER: 172.25.128.1#53(172.25.128.1) (UDP)
;; WHEN: Fri Oct 25 18:31:14 +07 2024
;; MSG SIZE rcvd: 224

nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~$ host -t mx uit.edu.vn
uit.edu.vn mail is handled by 40 aspmx2.googlemail.com.
uit.edu.vn mail is handled by 20 alt2.aspmx.l.google.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.
uit.edu.vn mail is handled by 10 aspmx.l.google.com.
nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~$ |
```

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?

```
nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~$ host idontexist.uit.edu.vn
idontexist.uit.edu.vn has address 118.69.123.140
idontexist.uit.edu.vn has address 45.122.249.78
nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~$ host noexist.uit.edu.vn
noexist.uit.edu.vn has address 118.69.123.140
noexist.uit.edu.vn has address 45.122.249.78
nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~$ host baithuchanhso2.uit.edu.vn
baithuchanhso2.uit.edu.vn has address 45.122.249.78
baithuchanhso2.uit.edu.vn has address 118.69.123.140
nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~$ host www.uit.edu.vn
www.uit.edu.vn has address 118.69.123.140
www.uit.edu.vn has address 45.122.249.78
nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~$ |
```

Nhận xét: Kết quả trả về luôn giống nhau cho các hostname không tồn tại của tên miền uit.edu.vn

Giải thích: Máy chủ DNS của tên miền được cấu hình để trả về một địa chỉ IP mặc định (là địa chỉ IP của máy chủ) khi subdomain không tồn tại được yêu cầu. Các subdomain không hợp lệ sẽ được ánh xạ tới một địa chỉ IP cố định, thay vì trả về thông báo lỗi không tồn tại (NXDOMAIN).

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

Sử dụng rockyou.txt để tìm kiếm các hostname hợp lệ khác của megacorpone.com:

- Tạo script với đoạn code sau và thực thi:

The screenshot shows a terminal window with the following content:

```
File Edit Selection View Go Run Terminal Help ← → ⌘ nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~$ cd ATTT
ATTT > $ lab01_22.sh
1 #!/bin/bash
2
3 for ip in $(cat rockyou.txt); do
4     host $ip.megacorpone.com;
5 done
```

The terminal also displays the command history:

```
nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~$ cd ATTT
nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ chmod +x lab01_22.sh
nguyentransaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ ./lab01_22.sh
```

- Kết quả:

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
Host beautiful.megacorpone.com not found: 3(NXDOMAIN)
Host mylove.megacorpone.com not found: 3(NXDOMAIN)
Host angela.megacorpone.com not found: 3(NXDOMAIN)
Host poohbear.megacorpone.com not found: 3(NXDOMAIN)
Host patrick.megacorpone.com not found: 3(NXDOMAIN)
Host iloveme.megacorpone.com not found: 3(NXDOMAIN)
Host sakura.megacorpone.com not found: 3(NXDOMAIN)
Host adrian.megacorpone.com not found: 3(NXDOMAIN)
Host alexander.megacorpone.com not found: 3(NXDOMAIN)
Host destiny.megacorpone.com not found: 3(NXDOMAIN)
Host christian.megacorpone.com not found: 3(NXDOMAIN)
Host 121212.megacorpone.com not found: 3(NXDOMAIN)
Host sayang.megacorpone.com not found: 3(NXDOMAIN)
Host america.megacorpone.com not found: 3(NXDOMAIN)
Host dancer.megacorpone.com not found: 3(NXDOMAIN)
Host monica.megacorpone.com not found: 3(NXDOMAIN)
Host richard.megacorpone.com not found: 3(NXDOMAIN)
Host 112233.megacorpone.com not found: 3(NXDOMAIN)
Host princess1.megacorpone.com not found: 3(NXDOMAIN)
Host 555555.megacorpone.com not found: 3(NXDOMAIN)
Host diamond.megacorpone.com not found: 3(NXDOMAIN)
Host carolina.megacorpone.com not found: 3(NXDOMAIN)
Host steven.megacorpone.com not found: 3(NXDOMAIN)
Host rangers.megacorpone.com not found: 3(NXDOMAIN)
Host louise.megacorpone.com not found: 3(NXDOMAIN)
Host orange.megacorpone.com not found: 3(NXDOMAIN)
Host 789456.megacorpone.com not found: 3(NXDOMAIN)
Host 999999.megacorpone.com not found: 3(NXDOMAIN)
```

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, hemier.edu.vn, vnuhcm.edu.vn) và thực hiện zone transfer ứng với các nameserver đã tìm được.

Bước 1: Tạo script với đoạn code sau

```

$ lab01_23.sh ×

ATTT > $ lab01_23.sh
1 #!/bin/bash
2
3 # Danh sách các tên miền
4 domains=(
5   "hcmus.edu.vn"
6   "hcmussh.edu.vn"
7   "uit.edu.vn"
8   "hcmut.edu.vn"
9   "hcmiu.edu.vn"
10  "uel.edu.vn"
11  "hcmier.edu.vn"
12  "vnuhcm.edu.vn"
13 )
14
15 # Tạo một tệp tin để lưu nameserver
16 ns_file="nameservers.txt"
17
18 # Liệt kê nameserver cho từng tên miền
19 for domain in "${domains[@]}"; do
20   ns=$(dig NS "$domain" +short)
21
22   # Ghi vào tệp tin
23   if [ -n "$ns" ]; then
24     echo "$domain:" >> "$ns_file"
25     echo "$ns" >> "$ns_file"
26   fi
27 done
28
29 # Thực hiện zone transfer
30 while read -r line; do
31   # Lấy tên miền và nameserver
32   domain=$(echo "$line" | cut -d: -f1)
33   nameservers=$(echo "$line" | cut -d: -f2-)
34
35   for ns in $nameservers; do
36     axfr=$(dig AXFR "$domain" @"$ns" 2>/dev/null)
37   done
38 done < "$ns_file"
39

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```

; <>> DIG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> AXFR vnuserv.vnuhcm.edu.vn. @vnuserv.vnuhcm.edu.vn.
;; global options: +cmd
;; Transfer failed.
○ nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ □

```

Bước 2: Thực thi script vừa tạo

```

, TRANSFER FAILED.
● nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ chmod +x lab01_23.sh
● nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ ./lab01_23.sh
○ nguyentranbaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ □

```

Kết quả (trong file nameservers.txt):

```

$ lab01_23.sh      nameservers.txt X
ATTT > nameservers.txt
1 hcmus.edu.vn:
2 server.hcmus.edu.vn.
3 dns2.hcmus.edu.vn.
4 hcmussh.edu.vn:
5 ns2.vdconline.vn.
6 ns1.vdconline.vn.
7 uit.edu.vn:
8 ns2.pavietnam.vn.
9 nsbak.pavietnam.net.
10 ns1.pavietnam.vn.
11 hcmut.edu.vn:
12 dns4.hcmut.edu.vn.
13 dns1.hcmut.edu.vn.
14 dns2.hcmut.edu.vn.
15 dns3.hcmut.edu.vn.
16 hcmiu.edu.vn:
17 hcm-server1.vnn.vn.
18 vdc-hn01.vnn.vn.
19 uel.edu.vn:
20 ns1.dns.net.vn.
21 ns2.dns.net.vn.
22 hcmier.edu.vn:
23 server.vnuhcm.edu.vn.
24 vnuserv.vnuhcm.edu.vn.
25 vnuhcm.edu.vn:
26 ns2.vdc2.vn.
27 ns1.vdc2.vn.
28 server.vnuhcm.edu.vn.
29 vnuserv.vnuhcm.edu.vn.
30 |

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```

;; global options: +cmd
; Transfer failed.
● nguyentrabaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ chmod +x lab01_23.sh
● nguyentrabaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ ./lab01_23.sh
○ nguyentrabaoanh-22520066@LAPTOP-BPN8GDKT:~/ATTT$ 

```

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

Tên	Mô tả
std	Thực hiện các truy vấn DNS tiêu chuẩn (A, AAAA, MX, NS, SOA)
all	Thực hiện tất cả các loại truy vấn có sẵn
brt	Thực hiện brute-force để tìm subdomain
ns	Truy vấn các bản ghi NS (Name Server)
mx	Truy vấn các bản ghi MX (Mail Exchange)
txt	Truy vấn các bản ghi TXT
srv	Truy vấn các bản ghi SRV (Service Records)
ptr	Truy vấn các bản ghi PTR (Pointer, dùng trong reverse DNS lookup)
soa	Truy vấn bản ghi SOA (Start of Authority)
axfr	Thực hiện zone transfer

zsk	Truy vấn các bản ghi DNSSEC Zone Signing Key
crt	Truy vấn thông tin chứng chỉ SSL/TLS từ các nguồn công khai (CRT.sh)
rvl	Thực hiện reverse lookup (truy vấn ngược từ IP để lấy tên miền)

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

- Reverse Lookup kết hợp brute force subdomain và lưu kết quả ra file JSON

Lệnh: dnsrecon -d mydomain.com -t rvl -b -j output.json

- Truy vấn các bản ghi TXT và MX, xuất kết quả ra file CSV

Lệnh: dnsrecon -d mydomain.com -t txt,mx -c results.csv

- Brute Force subdomain với từ điển tùy chỉnh và lưu kết quả ra file XML

Lệnh: dnsrecon -d mydomain.com -t brt -D customlist.txt -x subdomains.xml

- Thực hiện truy vấn NS và kiểm tra Zone Transfer, lưu kết quả ra file CSV

Lệnh: dnsrecon -d mydomain.com -t ns,axfr -c ns_axfr results.csv

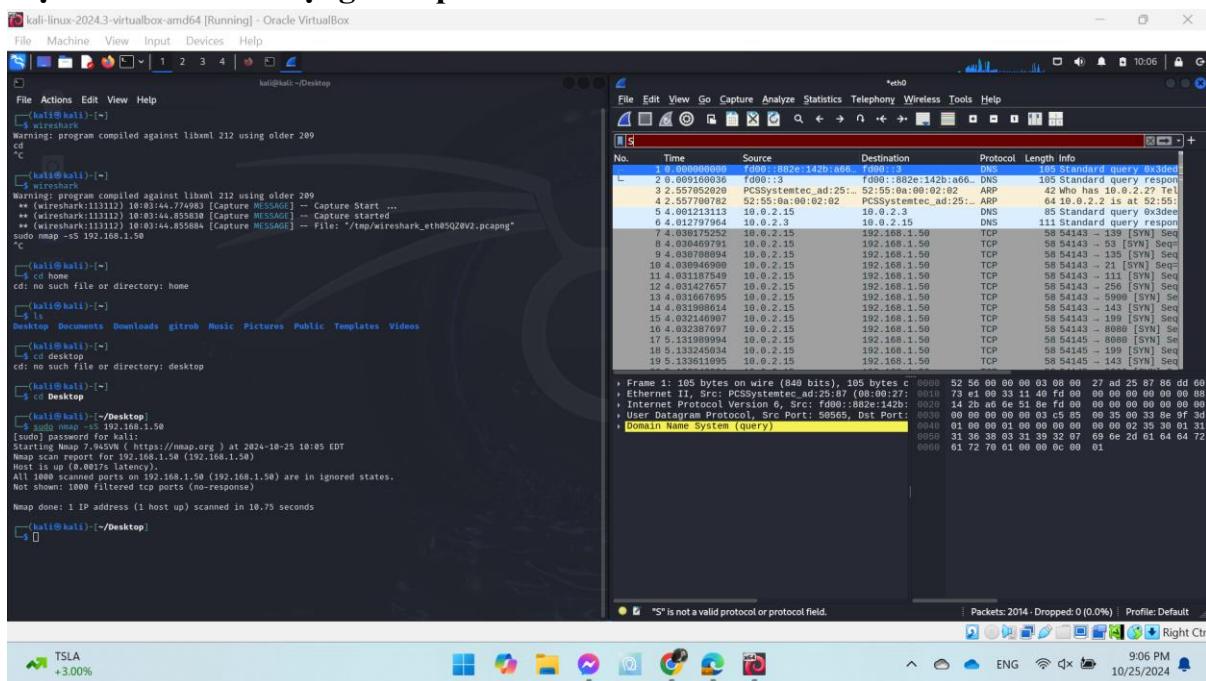
26. So sánh 2 công cụ DNSEnum và DNSRecon? Công cụ nào dễ sử dụng hơn?

Công cụ nào cho kết quả chính xác hơn? Công cụ nào hiển thị nhiều kết quả hơn?

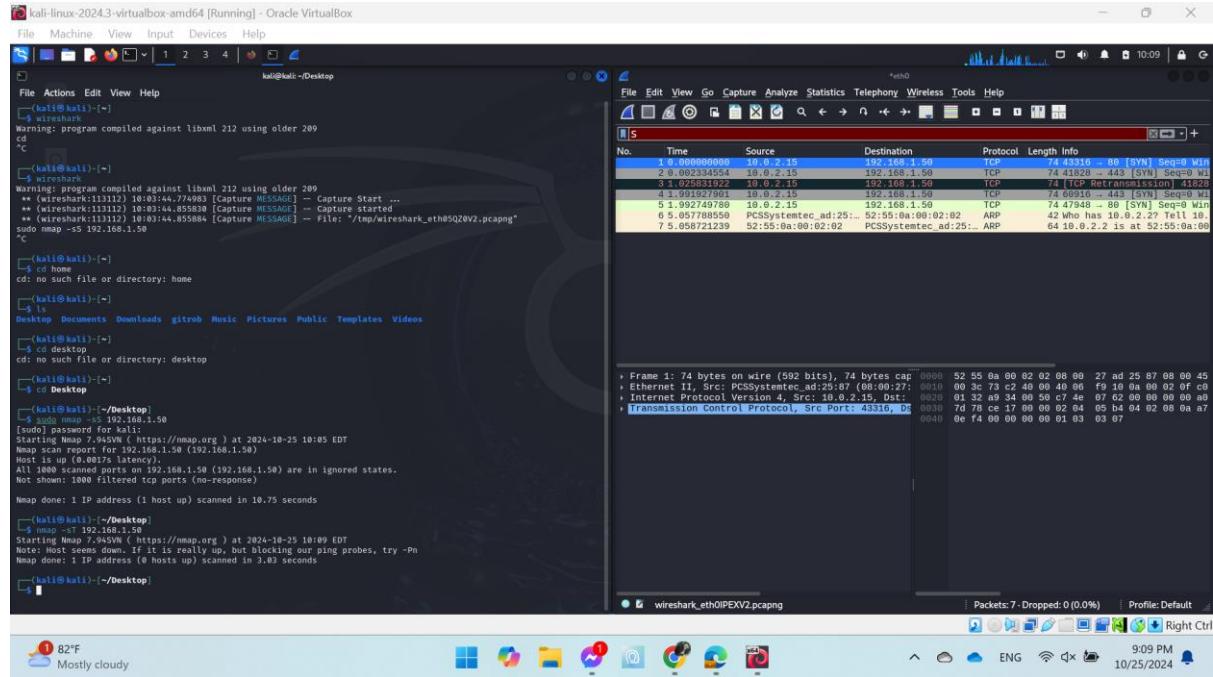
Tính năng	DNSEnum	DNSRecon
Độ dễ sử dụng	Dễ sử dụng, có cú pháp đơn giản, ít tùy chọn. Phù hợp với người mới bắt đầu.	Cần cấu hình nhiều tùy chọn hơn, phù hợp cho người dùng có kinh nghiệm.
Độ chính xác	Độ chính xác cao khi brute-force subdomain.	Cung cấp kết quả chi tiết, hỗ trợ nhiều loại truy vấn (A, MX, SOA, SRV, DNSSEC), giúp tăng độ chính xác.
Kết quả	<ul style="list-style-type: none"> Kết quả thường hiển thị trên màn hình terminal dưới dạng văn bản (text). Không hỗ trợ trực tiếp xuất kết quả ra file. Người dùng phải sử dụng cách redirect output (ví dụ: >) để lưu kết quả. 	<ul style="list-style-type: none"> Hỗ trợ nhiều định dạng kết quả khác nhau: JSON (-j): Xuất kết quả ra file JSON. CSV (-c): Xuất kết quả ra file CSV. XML (-x): Xuất kết quả ra file XML.

		XML. - Hiển thị trực tiếp trên terminal dưới dạng văn bản chi tiết.
Tùy chọn	Ít tùy chọn, chủ yếu tập trung vào brute-force và reverse lookup.	Nhiều tùy chọn, bao gồm truy vấn nhiều loại bản ghi, kiểm tra DNSSEC, zone transfer, và brute-force subdomain.
Loại thông tin DNS thu thập	Tên miền phụ, máy chủ DNS	Tên miền phụ, máy chủ DNS, bản ghi A, MX, TXT, NS, SOA, PTR, SRV, RP, NAPTR
Tính năng đặc biệt	Tập trung vào brute-force và zone transfer, ít tính năng mở rộng.	Hỗ trợ truy vấn DNSSEC, kiểm tra Zone Transfer, lưu kết quả ra nhiều định dạng (JSON, CSV, XML).

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



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

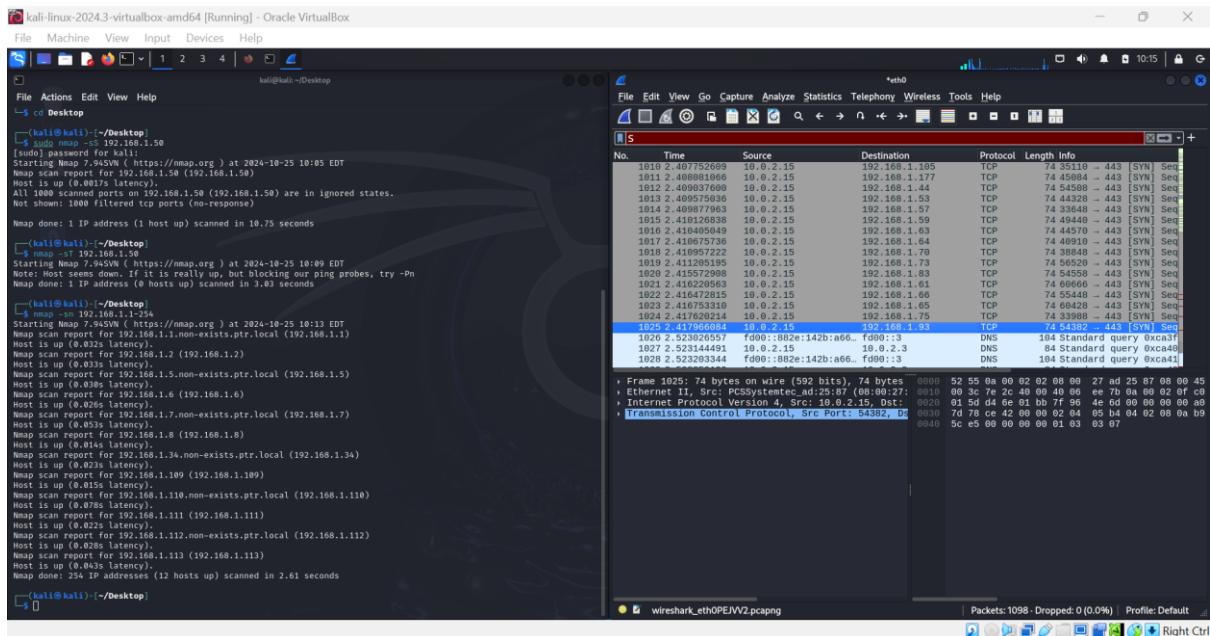


29. So sánh với sử dụng phương thức SYN Scan (số lượng gói tin được gửi, số lượng gói tin được nhận, thời gian quét, kết quả hiển thị...)

Scan Post	SYN Scan (Nmap -sS)	Connect Scan (Nmap -sT)
Phương pháp quét công	-sS	-sT
Số lượng gói tin gửi	Gửi ít gói tin hơn do chỉ gửi gói SYN.	Gửi nhiều gói tin hơn do hoàn thành cả quá trình kết nối TCP (SYN, SYN-ACK, ACK)
Số lượng gói tin nhận	Nếu cổng mở: nhận 1 gói SYN-ACK và không gửi gói ACK. Nếu cổng đóng: nhận 1 gói RST.	Nếu cổng mở: nhận 1 gói SYN-ACK và sau đó gửi 1 gói ACK để hoàn tất kết nối. Nếu cổng đóng: nhận 1 gói RST.
Thời gian quét	Thời gian quét thường nhanh hơn do không hoàn tất ba bước bắt tay TCP.	Chậm hơn do phải hoàn tất quá trình bắt tay TCP (SYN, SYN-ACK, ACK) và đóng kết nối.

Kết quả hiển thị	Hiển thị các port mở, đóng, hoặc được lọc. Port open khi nhận SYN-ACK , port closed khi nhận RST .	Hiển thị các port mở, đóng, hoặc được lọc. Port open khi kết nối thành công (hoàn tất handshake).
Phát hiện	Khó bị phát hiện hơn, thường được coi là quét nửa mở (half-open), không hoàn tất kết nối nên ít gây chú ý.	Dễ bị phát hiện hơn vì hoàn tất kết nối TCP đầy đủ, để lại dấu vết rõ ràng hơn trong log của server.

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



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