

# BÁO CÁO THỰC HÀNH

Môn học: An Toàn Mạng

Tên chủ đề: Information Gathering

GVHD: Tô Trọng Nghĩa

Nhóm: 3

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT140.P11.ANTT.1

STT	Họ và tên	MSSV	Email
1	Hà Minh Quân	22521177	22521177@gm.uit.edu.vn
2	Tù Chí Kiên	22520713	22520713@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng	Trang
1	Thực hiện theo hướng dẫn	100%	
2	Bài tập yêu cầu	100%	
3	Bài tập cộng điểm	...	...
Điểm tự đánh giá			?/10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

A.	Do thám Website (Website Reconnaissance).....	2
B.	Whois Enumeration.....	3
C.	Google Hacking.....	7
D.	Netcraft .....	11
E.	Recon-ng.....	12
F.	Open-Source Code.....	27
G.	Shodan.....	28
H.	theHarvester.....	30
I.	Information Gathering Frameworks.....	32
J.	DNS Enumeration .....	35
K.	Port Scanning.....	47

## A. Do thám Website (Website Reconnaissance)

<sup>®</sup> Bài tập về nhà (yêu cầu làm)

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

MegaCorp One specializes in disruptive innovation in the nanotechnology industry. We are responsible for industry defining standards in the medical, electronic, and commerce fields.

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)?

### a) MEET OUR TEAM

### MEET OUR TEAM

**Joe Sheer**  
**CHIEF EXECUTIVE OFFICER**  
Email: [joe@megacorpone.com](mailto:joe@megacorpone.com)  
Twitter: [@Joe\\_Sheer](https://twitter.com/Joe_Sheer)

**Tom Hudson**  
**WEB DESIGNER**  
Email: [thudson@megacorpone.com](mailto:thudson@megacorpone.com)  
Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)

**Tanya Rivera**  
**SENIOR DEVELOPER**  
Email: [trivera@megacorpone.com](mailto:trivera@megacorpone.com)  
Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)

**Matt Smith**  
**MARKETING DIRECTOR**  
Email: [msmith@megacorpone.com](mailto:msmith@megacorpone.com)  
Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)

#### 1. Name : **Joe Sheer**

Position : CHIEF EXECUTIVE OFFICER

Email : [joe@megacorpone.com](mailto:joe@megacorpone.com)

Twitter: [@Joe\\_Sheer](https://twitter.com/Joe_Sheer)

#### 2. Name : **Tom Hudson**

Position: Web Designer

Email: [thudson@megacorpone.com](mailto:thudson@megacorpone.com)

Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)

#### 3. Name: **Tanya Rivera**

Position: SENIOR DEVELOPER

Email: [trivera@megacorpone.com](mailto:trivera@megacorpone.com)

Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)

#### 4. Name: **Matt Smith**

Position: MARKETING DIRECTOR

Email: [msmith@megacorpone.com](mailto:msmith@megacorpone.com)

Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)

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

Cấu trúc email của tổ chức này được xây dựng trên nguyên tắc tên viết tắt của họ và tên đầy đủ của nhân viên, kèm theo tên miền của công ty (ví dụ: "thudson@megacorpone.com").

## B. Whois Enumeration

**Whois** là 1 dịch vụ TCP, công cụ, loại CSDL có thể cung cấp thông tin về tên miền như: Name servers (địa chỉ DNS đang trả về của tên miền), registrar (nhà quản lý tên miền, thường là các tổ chức, tập đoàn phân phối tên miền theo đuôi tên miền như Verisign, Mắt Bão, Namecheap, Godaddy, ...), ngày đăng ký tên miền...

```
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: 2024-10-04T02:05:44Z <<<

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
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and  
Registrars.  
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: 2013-01-22T22:01:00Z  
Registrar Registration Expiration 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  
Reseller:  
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited  
Domain Status:  
Domain Status:  
Domain Status:  
Domain Status:  
Registry Registrant ID:  
Registrant Name: Alan Grofield ←  
Registrant Organization: MegaCorpOne  
Registrant Street: 2 Old Mill St  
Registrant City: Rachel  
Registrant State/Province: Nevada  
Registrant Postal Code: 89001  
Registrant Country: US  
Registrant Phone: +1.9038836342  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net  
Registry Admin ID:  
Admin Name: Alan Grofield
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Ở đây cho ta biết được **Alan Grofield** là người đăng ký tên miền

```

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 } ← Name
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-04T02:05:44Z <<<

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

```

Các name server đang quản lý tên miền megacorpone.com

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?

```

File Actions Edit View Help
└─(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

└─(kali㉿kali)-[~]
$ 

```

Hiện như trên là do tên miền .vn chặn và không cho truy cập. và cũng có thể tên miền quốc gia có thể chọn cách cung cấp dịch vụ WHOIS khác nhau.

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

KIỂM TRA TÊN MIỀN

uit.edu.vn

Kiểm tra

Thông tin WHOIS tên miền

**uit.edu.vn**

Tên miền: uit.edu.vn

Ngày đăng ký: 02-10-2006

Ngày hết hạn: 02-10-2029

Chủ sở hữu tên miền: Trường Đại học Công nghệ Thông tin

Còn trạng thái: clientTransferProhibited

Quản lý tại Nhà đăng ký: Công ty TNHH PA Việt Nam

Nameservers: ns1.pavietnam.vn, ns2.pavietnam.vn, nsbak.pavietnam.net

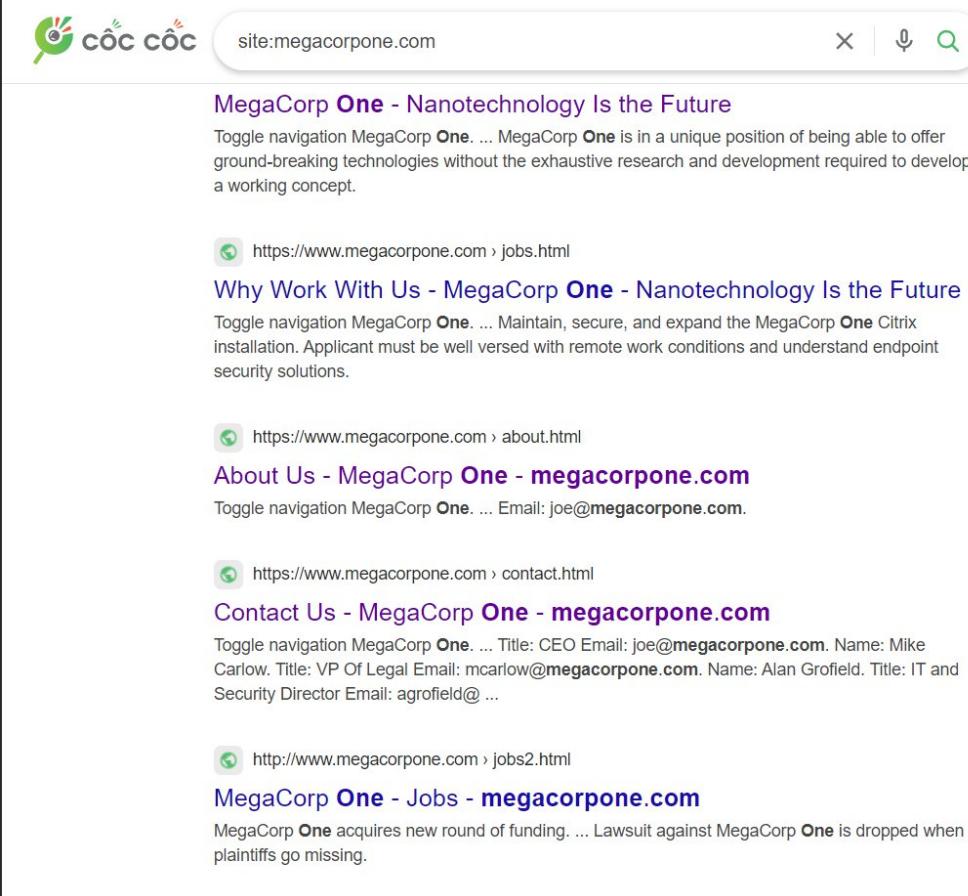
DNSSEC: unsigned

Ta có thể truy cập vào web <https://whois.inet.vn/> để kiểm tra

- Ngày đăng ký tên miền : 02-10-2006
- Ngày hết hạn : 02-10-20229
- Chủ sở hữu : Trường đại học Công Nghệ Thông Tin
- Các Name Sever:
  - ns1.pavietnam.vn
  - ns2.pavietnam.vn
  - nsbak.pavietnam.net

## C. Google Hacking

Thuật ngữ “Google Hacking” trở nên phổ biến bởi Jonny Long vào năm 2001. Ông ấy đã chỉ ra cách sử dụng các search engine như Google có thể lấy được các thông tin, lỗ hổng quan trọng của các website cấu hình sai. Hãy thử một vài từ khóa cơ bản. Từ khóa **site** chỉ thực hiện tìm kiếm trên một tên miền nhất định



The screenshot shows a Cốc Cốc browser window with the search bar containing "site:megacorpone.com". Below the search bar, there are several search results:

- MegaCorp One - Nanotechnology Is the Future**  
Toggle navigation MegaCorp One. ... MegaCorp One is in a unique position of being able to offer ground-breaking technologies without the exhaustive research and development required to develop a working concept.  
<https://www.megacorpone.com › jobs.html>
- Why Work With Us - MegaCorp One - Nanotechnology Is the Future**  
Toggle navigation MegaCorp One. ... Maintain, secure, and expand the MegaCorp One Citrix installation. Applicant must be well versed with remote work conditions and understand endpoint security solutions.  
<https://www.megacorpone.com › about.html>
- About Us - MegaCorp One - megacorpone.com**  
Toggle navigation MegaCorp One. ... Email: joe@megacorpone.com.  
<https://www.megacorpone.com › contact.html>
- Contact Us - MegaCorp One - megacorpone.com**  
Toggle navigation MegaCorp One. ... Title: CEO Email: joe@megacorpone.com. Name: Mike Carlow. Title: VP Of Legal Email: mcarlow@megacorpone.com. Name: Alan Grofield. Title: IT and Security Director Email: agrofield@ ...  
<http://www.megacorpone.com › jobs2.html>
- MegaCorp One - Jobs - megacorpone.com**  
MegaCorp One acquires new round of funding. ... Lawsuit against MegaCorp One is dropped when plaintiffs go missing.

Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstraw0
2024-08-23	ext:nix "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstraw0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoraram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl:"/portal/portal.mwsl"	Vulnerable Servers	Kishoraram
2024-07-04	Google Dork Submision For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id"   intext:"aws_secret_access_key" filetype:json   filetype:yaml	Files Containing Passwords	Joel Indra
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2024-07-04	site:.edu filetype:xls "root" database	Files Containing Juicy Info	defaltredmode
2024-07-04	inttitle:index of /etc/ssh	Files Containing Passwords	Shivam Dhingra
2024-05-13	"START test_database" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-13	"Header for logs at time" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-01	inttext:"dhcpd.conf" "index of"	Files Containing Juicy Info	Prathamesh Waidande

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

Name: Mike Carlow  
 Title: VP Of Legal  
 Email: [mcarlow@megacorpone.com](mailto: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](http://www.megacorpone.com)?

Profile	Name	Title	Location	LinkedIn URL	Action Buttons
Mutunga Muli	Mutunga Muli	Electrical Specialist	Nairobi County, Kenya	@megacorpone.com	<a href="#">Get Contact Info</a> <a href="#">View More</a>
Giovanni Kapo	Giovanni Kapo	Business Specialist	France	@megacorpone.com	<a href="#">Get Contact Info</a> <a href="#">View More</a>
Emac Oscp	Emac Oscp	Senior Tester	Deadwood, SD, US	Get contact info to view data	<a href="#">Get Contact Info</a> <a href="#">View More</a>
Steve Wong	Steve Wong	System Administrator	Vancouver, BC, CA	@megacorpone.com	<a href="#">Get Contact Info</a> <a href="#">View More</a>
Ga Rod	Ga Rod	Boss	Panama City Beach, FL, US	Get contact info to view data	<a href="#">Get Contact Info</a> <a href="#">View More</a>

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

Từ khóa thường gặp :

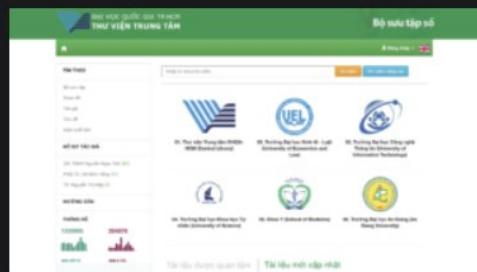
- “site” giới hạn tìm kiếm 1 trang website cụ thể nào đó .  
Ví dụ “site:github/.com “BEGIN OPENSSH PRIVATE KEY”
- “intext” tìm kiếm từ khóa trong nội dung của một trang web  
Ví dụ : intext: “ iphone 16”
- “Inurl” Tìm kiếm từ khóa trong URL của trang web.  
Ví dụ: inurl:cgi-bin/koha”
- “Intitle” tìm kiếm từ khóa trong tiêu đề của trang web  
Ví dụ: intitle:index of/etc/ssh
- “ext” giới hạn kết quả tìm kiếm trong các file

Ví dụ : [ext:nix "BEGIN OPENSSH PRIVATE KEY"](#)

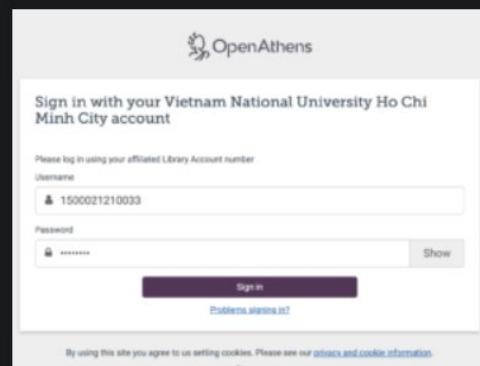
10. *Thực hiện tìm kiếm các tài liệu thú vị của Trường Đại học Công nghệ Thông tin mà được công bố trên Internet mà theo bạn là không nên được công bố?*

các lĩnh vực, các trưởng khác trong khối ĐHQG-HCM

**Bước 1.** Truy cập đường dẫn <https://ir.vnulib.edu.vn/>



**Bước 2:** Đăng nhập tài khoản sinh viên có dạng 15000 + MSSV (ví dụ: 1500023210000) và nhập mật khẩu (đăng nhập lần đầu mặc định là 12345678)



Công khai hướng dẫn đăng nhập vào tài khoản thư viện với mật khẩu mặc định là 12345678 thì có thể kẻ xâu tra MSSV của sinh và có thể đăng nhập và đổi mật khẩu qua các danh sách khen thưởng ví dụ như vinh danh sinh viên của trường

## D. Netcraft



## Hostnames matching .megacorpone.com

►  Search with another pattern?

alts

Site	First seen	Netblock	OS	Site Report
www.megacorpone.com	March 2013	OVH Hosting, Inc.	Linux - Debian	
support.megacorpone.com	May 2018	OVH Hosting, Inc.	unknown	
intranet.megacorpone.com		OVH Hosting, Inc.	unknown	
admin.megacorpone.com		OVH Hosting, Inc.	unknown	



### ⑤ Bài tập về nhà (Cộng điểm)

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

Network			
Site	http://www.megacorpone.com	Domain	megacorpone.com
Netblock Owner	OVH Hosting, Inc.	Nameserver	ns1.megacorpone.com
Hosting company	OVH	Domain registrar	gandi.net
Hosting country	CA	Nameserver organisation	whois.gandi.net
IPv4 address	149.56.244.87	VirusTotal	MegaCorpOne, Rachel, 89001, United States
IPv4 autonomous systems	A516276	DNS admin	admin@megacorpone.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled

Nameserver là ns1.megacorpone.com

## E. Recon-ng

thực hiện lệnh recon-ng. để bật recon-ng

```

kali㉿kali: ~
File Actions Edit View Help
[*] Version check disabled.

Sponsored by ...
^
^ \ \ ^ 
/ \ / \ \ \
// / \ \ \ \ \
www.blackhillsinfosec.com

PRACTISEC - helping you get your pages back
www.practisec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)] browsing session. Select Restore Session to try again.

[*] No modules enabled/installed. Not able to restore your session? Sometimes a tab is causing the issue. View previous tabs, remove the checkmark from the tabs you don't need to recover, and then restore.

[recon-ng][default] > marketplace search github

```

Sử dụng lệnh **marketplace search** để tìm kiếm các module của recon-ng.

```

[recon-ng][default] > marketplace search github
[*] Searching module index for 'github' ...

+-----+
|          Path           | Version | Status | Updated | D | K |
+-----+
| recon/companies-multi/github_miner | 1.1    | not installed | 2020-05-15 | | * |
| recon/profiles-contacts/github_users | 1.0    | not installed | 2019-06-24 | | * |
| recon/profiles-profiles/profiler | 1.2    | not installed | 2023-12-30 | |   |
| recon/profiles-repositories/github_repos | 1.1    | not installed | 2020-05-15 | | * |
| recon/repositories-profiles/github_commits | 1.0    | not installed | 2019-06-24 | | * |
| recon/repositories-vulnerabilities/github_dorks | 1.0    | not installed | 2019-06-24 | | * |
+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace info
Shows detailed information about available modules

Usage: marketplace info <>path>|<prefix>|all>

[recon-ng][default] > marketplace info
Shows detailed information about available modules

Usage: marketplace info <>path>|<prefix>|all>

```

```
[recon-ng][default] > marketplace info recon/companies-multi/github_miner
+-
| path      | recon/companies-multi/github_miner
| name      | Github Resource Miner
| author    | Tim Tomes (@lanmaster53)
| version   | 1.1
| last_updated | 2020-05-15
| description | Uses the Github API to enumerate repositories and member profiles associated with a company search string. Updates the respective table
s with the results.
| required_keys | ['github_api']
| dependencies | []
| files      | []
| status      | not installed
+-
```

Sử dụng **marketplace search netcraft** để tìm kiếm path để tải

```
[recon-ng][default] > marketplace search netcraft
[*] Searching module index for 'netcraft' ...
```

Path	Version	Status	Updated	D	K
recon/domains-hosts/netcraft	1.1	installed	2020-02-05		

Sau đó sử dụng **marketplace install recon/domains-host/netcraft** để tải module

```
[recon-ng][default] > marketplace install recon/domains-hosts/netcraft
[*] Module installed: recon/domains-hosts/netcraft
[*] Reloading modules ...
[recon-ng][default] >
```

Sử dụng module **recon/domains-hosts/netcraft**

```
[recon-ng][default] > modules load recon/domains-hosts/netcraft
[recon-ng][default][netcraft] > info

    Name: Netcraft Hostname Enumerator
    Author: thrapt (thrapt@gmail.com)
    Version: 1.1

Description:
    Harvests hosts from Netcraft.com. Updates the 'hosts' table with the results.

Options:
    Name      Current Value   Required  Description
    _____      _____       _____
    SOURCE    megacropone.com  yes        source of input (see 'info' for details)

Source Options:
    default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>     string representing a single input
    <path>       path to a file containing a list of inputs
    query <sql>   database query returning one column of inputs

[recon-ng][default][netcraft] > ]
```

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

MEGACORPONE.COM

```
[*] Searching Google for: site:megacorpone.com
[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 301.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 401.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 501.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 601.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 701.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 801.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 901.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1001.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1101.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1201.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1301.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1401.
[*] Searching Google for: site:megacorpone.com -site:www.megacorpone.com
```

Hình trên sử dụng lệnh **options set SOURCE megacorpone.com** để thiết lập tên miền của mục tiêu. Chạy lệnh **run** để chạy module

```
[recon-ng][default] > show hosts

+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+-----+
| 1 | www.megacorpone.com | | | | | | google_site_web |
+-----+
```

Sử dụng lệnh show hosts để xem lịch sử các host đã được tìm thấy.

**Bài tập về nhà (Yêu cầu làm)**

12. Thực hiện sử dụng module có thể giúp phân giải tên miền ở Hình 20 thành địa chỉ IP tương ứng.
13. Sử dụng một số module khác có trong recon-ng để thu thập thông tin về UIT nhiều nhất có thể.

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

```
[recon-ng][default] > marketplace install recon/hosts-hosts/resolve
[*] Module installed: recon/hosts-hosts/resolve
[*] Reloading modules ...
[recon-ng][default] > modules load recon/hosts-hosts/resolve
[recon-ng][default][resolve] > options set SOURCE megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][resolve] > run
```

Tải **resolve** và sử dụng lệnh **options set SOURCE megacorpone.com** để thiết lập tên miền của mục tiêu Chạy lệnh run để chạy module

```
[recon-ng][default][resolve] > run
[*] www.megacorpone.com => 149.56.244.87
[recon-ng][default][resolve] >
```

Và kết quả ip của [www.megacorpone.com](http://www.megacorpone.com) là 149.56.244.87

13. sử dụng các lệnh có như hướng dẫn ở trên và hiện lên 1 số thông tin như dưới

```
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][google_site_web] > info
  Name: Google Hostname Enumerator
  Author: Tim Tomes (@lanmaster53)
  Version: 1.0

  Description:
    Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
    the results.

  Options:
  Name   Current Value   Required   Description
  SOURCE  magecorpone.com  yes        source of input (see 'info' for details)

  Source Options:
  default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>   database query returning one column of inputs
```

Theo như kết quả sau khi khởi động recon-ng, chúng ta cần cài đặt module google\_site\_web để có thể sử dụng recon-ng. Chúng ta có thể thêm các module từ "Marketplace search" để tìm kiếm các module của recon-ng.

một số thông tin thu thập được về uit có 1 số host name như **inseclab.uit.edu.vn** host này là phòng thí nghiệm An Toàn Thông Tin

**thuvien.uit.edu.vn**

**dsc.uit.edu.vn** có thể xem 1 số ảnh dưới đây được recon-ng liệt kê

```
[*] Country: None
[*] Host: drc.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: nlp.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: qhdn.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

Theo như kết quả sau khi khởi động recon-ng, chúng ta cần cài đặt module marketplace search để có thể sử dụng recon-ng. Chúng ta có thể thêm các module từ "Marketplace search" để tìm kiếm các module của recon-ng.

```

UIT.EDU.VN

[*] Searching Google for: site:uit.edu.vn
[*] Country: None
[*] Host: inseclab.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: thuvien.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: khoahocitre.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: dsc.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None

```

Hình 12. Khởi động recon

Theo như kết quả sau khi khởi động recon để có thể sử dụng recon-ng. Chúng ta có thể thêm lệnh marketplace search để tìm kiếm các module.

```

Country: None
Host: congdoan.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None

```

```

Country: None
Host: dev.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None

```

Theo như kết quả sau khi khởi động recon để có thể sử dụng recon-ng. Chúng ta có thể thêm lệnh marketplace search để tìm kiếm các module.

```
Country: None
Host: nlp.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
```

```
Country: None
Host: qhdn.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
```

```
Country: None
Host: phongdl.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
```

Theo như kết quả sau k

```
[*] _____
[*] Country: None
[*] Host: tuyensinh.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] _____
[*] Country: None
[*] Host: vlab.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] _____
[*] Country: None
[*] Host: dbcl.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
Country: None
Host: ctgt.uit.edu.vn [Kali Docs] [Kali Forums] [Kali NetHunter]
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None

Country: None
Host: khmt.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None

Country: None
Host: fit.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None

Country: None
Host: tuyensinh.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None

Country: None
Host: vlab.uit.edu.vn
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
```

```
*] _____  
*] Country: None  
*] Host: rms.uit.edu.vn [Kali Docs] [Kali Forum] [Kali NetHunter] [E  
*] Ip_Address: None  
*] Latitude: None  
*] Longitude: None  
*] Notes: None  
*] Region: None  
*]  
*] Country: None  
*] Host: daihoiviii-tuoitre.uit.edu.vn  
*] Ip_Address: None  
*] Latitude: None  
*] Longitude: None  
*] Notes: None  
*] Region: None  
*]  
*] Country: None  
*] Host: tuoitre.uit.edu.vn  
*] Ip_Address: None  
*] Latitude: None  
*] Longitude: None  
*] Notes: None  
*] Region: None  
*]  
*] Country: None  
*] Host: www.uit.edu.vn  
*] Ip_Address: None  
*] Latitude: None  
*] Longitude: None  
*] Notes: None  
*] Region: None  
*]  
*] Country: None  
*] Host: mmlab.uit.edu.vn  
*] Ip_Address: None  
*] Latitude: None  
*] Longitude: None  
*] Notes: None  
*] Region: None  
*]  
*] Country: None  
*] Host: jobs.uit.edu.vn
```

```

[*] _____
[*] Country: None   Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB
[*] Host: daa.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: khcn.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: aiclub.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: danguy.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: tchc.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None

```

Hình 12.

Theo như kết quả sau khi khởi động có thể sử dụng recon-*ng*. Chúng ta có lệnh **marketplace search** để tìm kiếm

[recon-*ng*][default] > marketplace search github  
Searching module index for 'github'...

```

[*] Region: None
[*]
[*] Country: None
[*] Host: csv1.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: oms.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: banqlcs.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: chungthuc.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: courses.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None

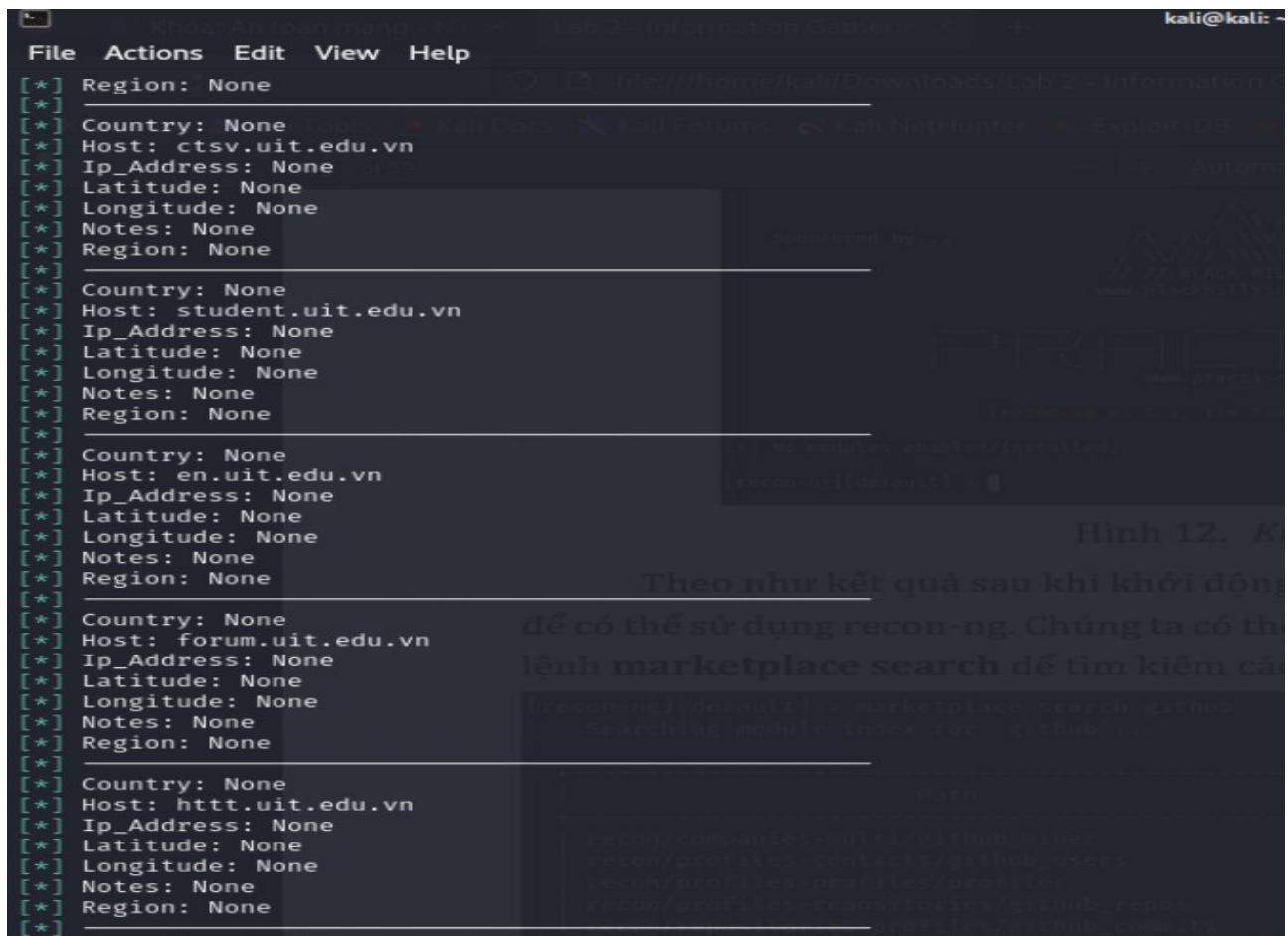
```

Hình 12. Kết quả sau khi khởi động recon-  
ng để có thể sử dụng recon-  
ng. Chúng ta có thể t  
hành lệnh marketplace search để tìm kiếm các n

[recon-ng][default]:> marketplace search github  
[recon-ng][default]:> searching module index for "github"...

```
[*] _____
[*] Country: None
[*] Host: oep.uit.edu.vn < Kali Docs < Kali Forums < Kali NetHunter < Exploit-DB < Google Hacking DB
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: link.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: mapr.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: cnsc.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: nc.uit.edu.vn
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: alumni.uit.edu.vn
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Hình 12. K

Theo như kết quả sau khi khởi động

dễ có thể sử dụng recon- ng. Chúng ta có thể lệnh **marketplace search** để tìm kiếm các

↳ [Search GitHub](#) | [Search Issues](#) | [Search Pull Requests](#)

Part 4

[recon/companies-matching-thru\\_repos](#)  
[recon/profiles-contacts-&-thru\\_repos](#)  
[recon/leads-contacts-&-thru\\_repos](#)

`git clone https://github.com/atom/hyperclick.git`

## F. Open-Source Code

The screenshot shows the GitHub profile page for the user 'megacorpone'. It features a large circular logo for 'MegaCorp One' with a blue and white design. Below the logo, the repository 'megacorpone.com' is listed as a public repository with 1 star, 30 forks, and 50 issues. Another repository, 'git-test', is also shown as public with 1 star, 3 forks, and 4 issues. A chart indicates 0 contributions in the last year. The contribution activity section for October 2024 shows no activity. The sidebar on the right lists years from 2017 to 2023.

Sau khi sử dụng từ khóa **file:users** để tìm kiếm các tập tin có chứa từ “**users**”. Thì ta đã tìm kiếm được tập tin xampp.users và trong tập tin này chứa tên đăng nhập và mật khẩu (dưới dạng mã hash).

The screenshot shows the GitHub repository page for 'megacorpone.com/xampp.users'. The left sidebar shows the repository structure with 'xampp.users' selected. The main pane displays the contents of the 'xampp.users' file, which contains a single line of text: 'trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3Gk54oUC0'. This is a hashed password entry.

### ® Bài tập về nhà (Cộng điểm)

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

## G. Shodan

Shodan là một search engine thu thập thông tin bất kỳ thiết bị nào được kết nối Internet, bao gồm các máy chủ web, các router, thiết bị IoT, ...

The screenshot shows the Shodan search results for the query 'vpn'. At the top, it displays 'TOTAL RESULTS' as 2,715,738. Below this are sections for 'TOP COUNTRIES' and 'TOP PORTS'. The 'TOP COUNTRIES' section lists Japan (680,899), China (440,030), United States (310,737), Australia (213,763), and Korea, Republic of (138,508). The 'TOP PORTS' section lists port 500 (2,591,441), port 4500 (62,807), port 443 (12,833), port 1723 (9,990), and port 161 (5,233). The main search results are displayed in two columns. The first result is for IP 213.90.51.90, which is a Network of Hutchison Drei Austria GmbH located in Austria, Vienna. It is identified as a 'VPN (IKE)' connection. The second result is for IP 77.100.51.85, which is a cpc125470-croy07-2-0-cust 84.19.2 cable virginia.net located in the United Kingdom, Wallington. It is also identified as a 'VPN (IKE)' connection. Both results show detailed network information such as Initiator SPI, Responder SPI, Next Payload, Version, Exchange Type, Flags, Encryption, Commit, Authentication, Message ID, and Length.

### Bài tập về nhà (Cộng điểm)

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.

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

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.

## Lab 02: Information Gathering

**TOTAL RESULTS**  
**3,166,213**

**TOP COUNTRIES**

Country	Count
China	496,962
United States	469,634
Korea, Republic of	260,402
Taiwan	156,752
Japan	153,915
More...	

**TOP PORTS**

Port	Count
1723	971,688
49152	468,871
9100	286,644
161	179,061
5.106.64.200	5.106.64.200

**3.34.217.123**

c-73-34-217-123.hsd1.co.c  
omcast.net  
Comcast IP Services,  
LLC  
United  
States, Englewood  
vpn

PPTP:  
Firmware: 1  
Hostname: local  
Vendor: Linux

2024-10-16T13:10:32.256

**150.243.162.22**

talk.truman.edu  
Truman State University  
United States, Kirksville

@RSYNCD: 31.0 sha512 sha256 sha1 md5 md4\ndebian  
ubuntu Ubuntu archive amd64 (https://www.debian.org/mirror/size)  
fedora-epe1 Extra Packages for Enterprise Linux  
webwork Webworks backups  
@RSYNCD: EXIT

2024-10-16T13:10:27.408

**115.237.98.236**

CHINANET-ZJ Shaoxing  
node network  
China, Shanghai

HTTP/1.1 500 Internal Server Error  
SERVER: Linux/2.6.21.5, UPnP/1.0, Portable SDK for UPnP devices/1.6.6  
CONNECTION: close  
CONTENT-LENGTH: 66  
CONTENT-TYPE: text/html

2024-10-16T13:10:27.085

**5.106.64.200**

2024-10-16T13:10:26.440

### Tìm kiếm sử dụng linux

**TOTAL RESULTS**  
**692,261**

**TOP COUNTRIES**

Country	Count
United States	474,508
China	36,883
India	23,742
Brazil	16,743
Japan	13,293
More...	

**TOP PORTS**

Port	Count
443	378,364
80	176,602
8649	29,445
3306	21,334

**35.227.194.149**

149.194.227.35.bc.googleusercontent.com  
Google LLC  
United States, Kansas City  
cloud

HTTP/1.1 200 OK  
Server: rhino-core-shield  
Date: Wed, 16 Oct 2024 13:12:16 GMT  
Content-Type: text/html; charset=UTF-8  
Vary: Accept-Encoding  
Expires: Thu, 01 Jan 1970 00:01:48 GMT  
Cache-Control: no-cache, private, no-transform, no-store  
Pragma: no-cache  
P3P: CP="IDC DSP COR ADM DEVi TAI1 PS..."

2024-10-16T13:16:46.641441

**34.111.147.58**

58.147.111.34.bc.googleusercontent.com  
Google LLC  
United States, Kansas City  
cloud

HTTP/1.1 404 Not Found  
Content-Type: application/xml; charset=UTF-8  
Content-Length: 127  
X-GUploader-UploadId: AHMUCY23\_ga-TdsN8fLnB6AHE1FBuY9FjTjGItk3fdnJX7fa8e1fh-i0sPH3yAqdT2lea3arFZwg  
Date: Wed, 16 Oct 2024 13:15:09 GMT  
Expires: Wed, 16 Oct 2024 13:15:09 GMT  
Cache-Control: private,...

2024-10-16T13:15:09.568678

**161.97.176.7**

vmd81025.contaboserver.net  
Contabo GmbH  
Germany, Düsseldorf

HTTP/1.1 200 OK  
Date: Wed, 16 Oct 2024 13:15:00 GMT  
Server: Apache/2.4.56 (Debian)

2024-10-16T13:15:00.280929

### Tìm kiếm với lệnh là google

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

Tính Năng	Shodan	Google,Bing
Mục tiêu tìm kiếm	Chuyên tìm kiếm thiết bị kết nối internet: máy chủ, camera, router, thiết bị IoT.	Tìm kiếm thông tin trên website, hình ảnh, video...
Dữ liệu thu thập	Thông tin kỹ thuật chi tiết về thiết bị: hệ điều hành, phiên bản phần mềm, cổng mở, dịch vụ đang chạy..	Nội dung trang web, meta dữ liệu, liên kết...
Cách thức hoạt động	Quét Internet để phát hiện các thiết bị trực tuyến và thu thập thông tin từ chúng.	Lập chỉ mục các trang web và sử dụng thuật toán để xếp hạng kết quả tìm kiếm
Thông tin về mạng và bảo mật	Chi tiết về IP, các cổng mở, phiên bản dịch vụ, thông tin về bảo mật (lỗ hổng, phần mềm cũ)	Không cung cấp chi tiết về các thiết bị mạng hoặc dịch vụ trực tiếp trên hệ thống.
Tính phức tạp	Cần có kiến thức về mạng và bảo mật để sử dụng hiệu quả.	Dễ sử dụng, giao diện thân thiện.
Công nghệ tìm kiếm	Quét và phân tích các cổng mở, thiết bị trực tuyến trên internet, thu thập dữ liệu trực tiếp từ các thiết bị, hệ thống, và dịch vụ chạy trực tuyến	Thu thập dữ liệu web từ nội dung trang web qua các bot tìm kiếm
Yêu cầu API key	Cần API key cho các truy vấn chuyên sâu và dữ liệu chi tiết.	Không yêu cầu API key cho truy vấn cơ bản (trừ khi sử dụng các dịch vụ tìm kiếm API)

## H. theHarvester

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ theHarvester -d megacorpone.com -b google
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*****
* [ _ _ _ | _ \ / _ ] / ^ / \ _ - _ \ \ / / _ \ v _ [ _ ] / _ \ _ _ | * 
* [ _ _ | _ \ / _ ] / ^ / \ _ - _ \ \ / / _ \ v _ [ _ ] / _ \ _ _ | * 
* [ _ _ | _ | _ | _ ] / ^ / \ _ - _ \ \ / / _ \ v _ [ _ ] / _ \ _ _ | * 
* [ \ _ _ | _ | _ | _ ] v _ / \ _ , _ | \ \ \ / \ _ \ \ / \ _ \ \ / \ _ | * 
* [ _ ] * 
* theHarvester 4.6.0 * 
* Coded by Christian Martorella * 
* Edge-Security Research * 
* cmartorella@edge-security.com * 
* [!] Invalid source.
```

Do theHarvester 4.6.0 không còn hỗ trợ trên google nữa:

```
-b SOURCE, --source SOURCE
    anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverun, brave,
    censys, certspotter, criminalip, crtsh, dnsdumpster, duckduckgo,
    fullhunt, github-code, hackertarget, hunter, hunterhow, intelx, netlas,
    onyphe, otx, penteestools, projectdiscovery, rapiddns, rocketreach,
    securityTrails, sitedossier, subdomaincenter, subdomainfinderc99,
    threatminer, tomba, urlscan, virustotal, yahoo, zoomeye
```

Sau khi sử dụng tất cả source được cung cấp thì đều cho ra kết quả sau:

```
(kali㉿kali)-[~/Documents/NT140/Lab02]$ theHarvester -d megacorpne.com -b brave
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*****
* [+] Trinh Kiem ^ Tim Kiem Brave   Tai soi lai kieu love   Tim kieu API *
* [+] Trinh Kiem ^ Tim Kiem Brave   Tai soi lai kieu love   Tim kieu API *
* [+] Trinh Kiem ^ Tim Kiem Brave   Tai soi lai kieu love   Tim kieu API *
* [+] Trinh Kiem ^ Tim Kiem Brave   Tai soi lai kieu love   Tim kieu API *
* [+] Trinh Kiem ^ Tim Kiem Brave   Tai soi lai kieu love   Tim kieu API *
* [+] Trinh Kiem ^ Tim Kiem Brave   Tai soi lai kieu love   Tim kieu API *
* [+] theHarvester 4.6.0           *
* Coded by Christian Martorella  *
* Edge-Security Research          *
* cmartorella@edge-security.com   *
*                                     *
*****
```

[\*] Target: megacorpne.com

An exception has occurred: 400, message:  
Can not decode content-encoding: br  
An exception has occurred: 400, message:  
Can not decode content-encoding: br  
An exception has occurred: 400, message:  
Can not decode content-encoding: br

[\*] Searching Brave.

[\*] No IPs found.

[\*] No emails found.

[\*] No hosts found.

## ⑧ Bài tập về nhà (Cộng điểm)

17. Sử dụng công cụ theHarvester để lấy tìm kiếm các địa chỉ email của UIT

Để truy cập uit.edu.vn thì nhập câu lệnh sau:

theHarvester -d uit.edu.vn -b yahoo

```
[*] Target: uit.edu.vn      Registrant Name: Trường Đại học Công  
[*] Searching Yahoo.        Registrar: Công ty TNHH PA VI  
[*] No IPs found.
```

Sau khi chạy sẽ xuất ra các email sau:

```

[*] Target: uit.edu.vn
[*] Searching Yahoo.
[*] No IPs found.
[*] Emails found: 47
alumni@uit.edu.vn
cbsvl@uit.edu.vn
ce@uit.edu.vn
chinhnt@uit.edu.vn
ttsv@uit.edu.vn
cuongvfk@uit.edu.vn
cuongvtk@uit.edu.vn
duyld@uit.edu.vn
hanhnt@uit.edu.vn
haodn@uit.edu.vn
hungmx@uit.edu.vn
huynq@uit.edu.vn
info.htt@uit.edu.vn
info.nc@uit.edu.vn
info@uit.edu.vn
inseclab@uit.edu.vn

```

18. Sử dụng với nguồn tìm kiếm khác (-b). Theo bạn, kết quả của nguồn nào tốt hơn?

Bảng phân tích nguồn:

Tên nguồn	Số IP	Số Email	Số Host	Note
baidu	0	14	1	
Bing	0	2	18	
crtsh	0	0	32	
dnsdumpster	0	0	75	
duckduckgo	0	1	67	
hackertarget	0	0	84	
otx	11	1	50	Nhiều ip nhất
rapiddns	0	0	388	Nhiều host nhất
subdomaincenter	0	0	71	
threatminer	1	0	0	
urlscan	6	0	9	Số ASNS:2 Số url: 17
Yahoo	0	47	52	Nhiều email nhất

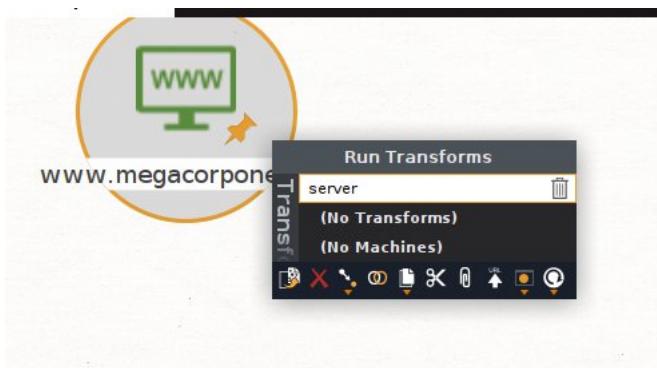
Những nguồn Anubis, bingapi, brave, certspotter, sitedossier, subdomainfinderc99 không trả về gì.

Những nguồn còn lại thiếu apikey.

Vậy theo bảng trên thì tùy người dùng muốn thông tin nào thì sử dụng nguồn tương ứng.

## I. Information Gathering Frameworks

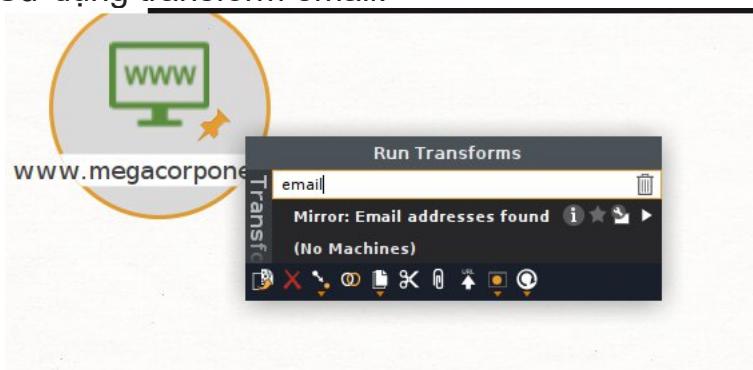
Sau khi làm theo hướng dẫn thì không tồn tại transform server technology



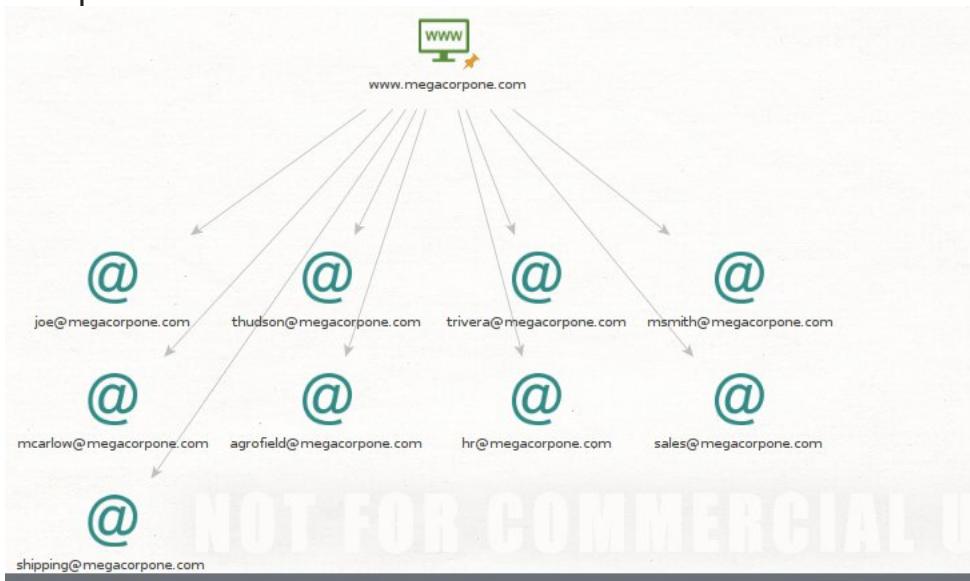
④ Bài tập về nhà (Yêu cầu làm)

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

Sử dụng transform email:



Kết quả transformation:



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

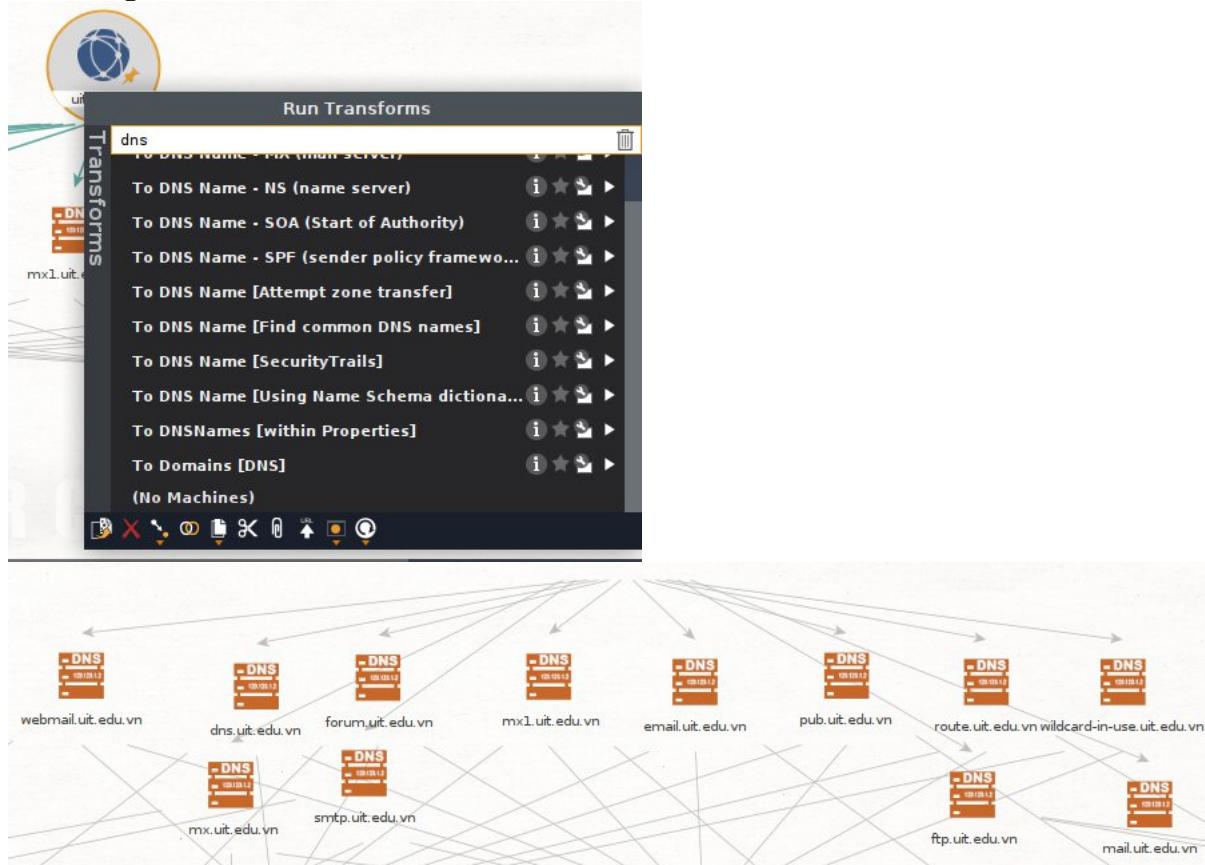
- Các bản ghi DNS.
- Các website và địa chỉ IP tương ứng.

a. Các bản ghi DNS.

Tạo một internet domain:

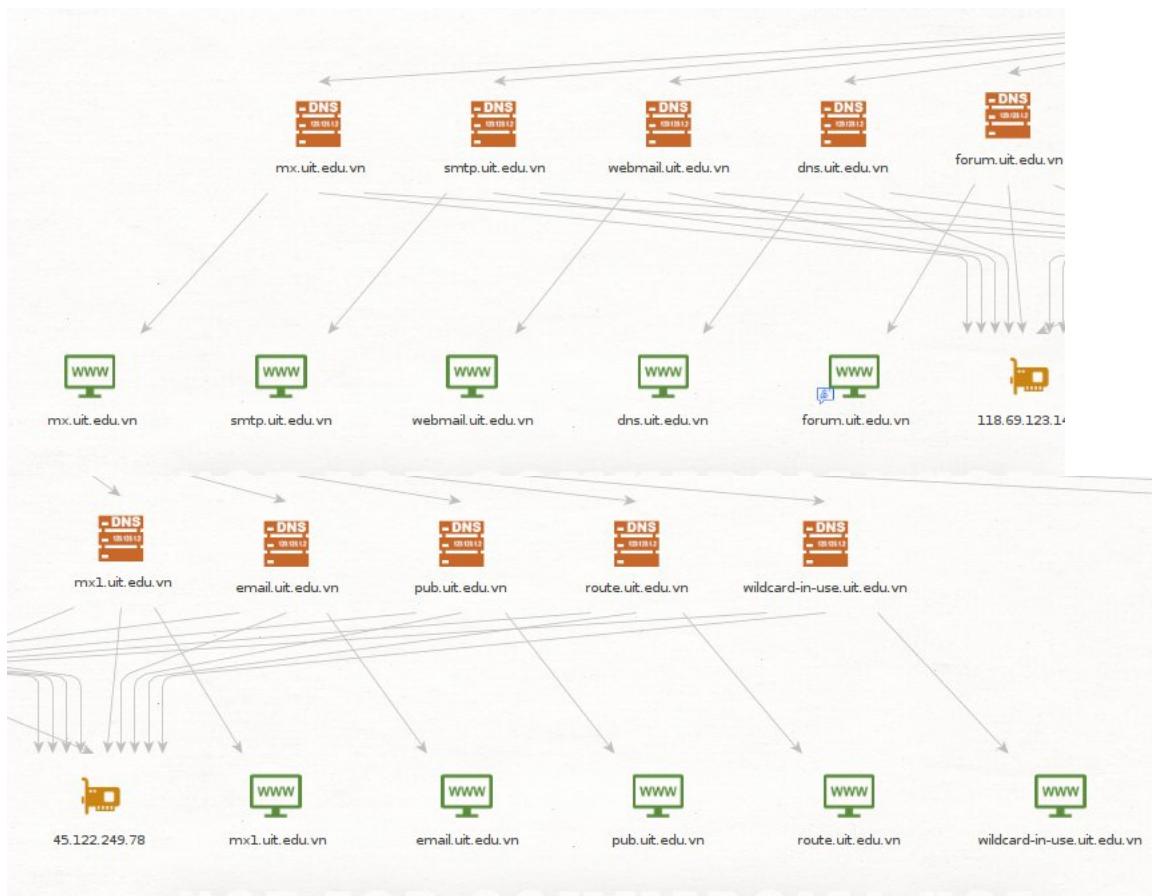


Sử dụng transformation Common Dns name:

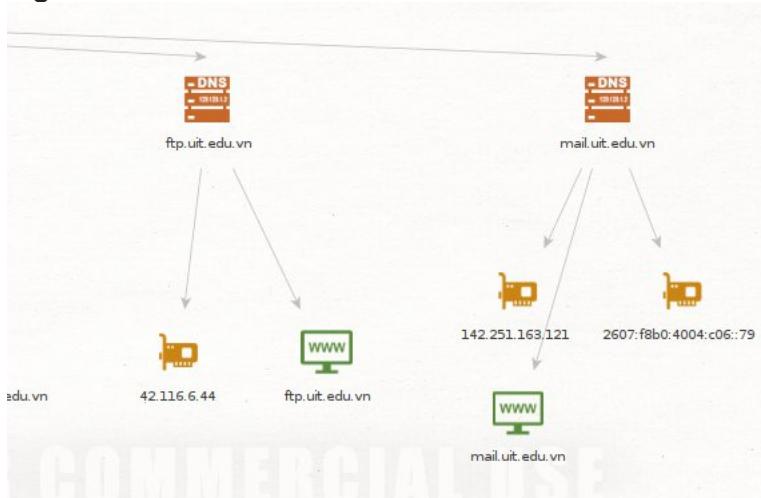


b. Các website và địa chỉ IP tương ứng:

Các tên miền sau có một website tương ứng và đều có cùng 2 địa chỉ ip giống nhau.



Ngoài ra còn có



## J. DNS Enumeration

Tương tác với máy chủ DNS

Sử dụng lệnh **host** để tìm địa chỉ IP của [www.megacorpone.com](http://www.megacorpone.com)

```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ host www.megacorpone.com
www.megacorpone.com has address 149.56.244.87
[(kali㉿kali)-[~]]$
```

Sử dụng lệnh host để tìm kiếm các bản ghi TXT và MX cho tên miền

```
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t txt www.megacorpone.com
www.megacorpone.com has no TXT record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t mx www.megacorpone.com
www.megacorpone.com has no MX record
```

### ⑧ Bài tập về nhà (Yêu cầu làm)

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

Ví dụ: a, aaaa, cname, ns, soa, srv, ptr, caa, ds, dnskey

```
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t a www.megacorpone.com
www.megacorpone.com has address 149.56.244.87
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t aaaa www.megacorpone.com
www.megacorpone.com has no AAAA record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t cname www.megacorpone.com
www.megacorpone.com has no CNAME record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t ns www.megacorpone.com
www.megacorpone.com has no NS record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t soa www.megacorpone.com
www.megacorpone.com has no SOA record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t srv www.megacorpone.com
www.megacorpone.com has no SRV record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t ptr www.megacorpone.com
www.megacorpone.com has no PTR record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$
```

```
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t caa www.megacorpone.com
www.megacorpone.com has no CAA record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t ds www.megacorpone.com
www.megacorpone.com has no DS record
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ host -t dnskey www.megacorpone.com
www.megacorpone.com has no DNSKEY record
```

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

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ host -t txt uit.edu.vn
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C91tPny8NLttGS0aU5pJjKiY"
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"
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"
uit.edu.vn descriptive text "k6t321pqvf9jryb0z4n5scftqph6t781"
uit.edu.vn descriptive text ".ukan9w1l3iica61scp6fwumq5v6dopw"
uit.edu.vn descriptive text "svp60rjlwr6s19rn9t013cfwm3xmqx7h"
```

host -t mx uit.edu.vn

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ 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 alt1.aspmx.l.google.com.
uit.edu.vn mail is handled by 10 aspmx.l.google.com.
uit.edu.vn mail is handled by 20 alt2.aspmx.l.google.com.
uit.edu.vn mail is handled by 40 aspmx3.googlemail.com.
```

### Tra cứu tự động (Automating Lookups)

```
(root㉿kali)-[/home/kali]
# host www.megacorpone.com
www.megacorpone.com has address 149.56.244.87

(root㉿kali)-[/home/kali]
# host noexist.megacorpone.com
Host noexist.megacorpone.com not found: 3(NXDOMAIN)
```

#### ④ Bài tập về nhà (Yêu cầu làm)

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?*

Kết quả trả về:

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ 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

(kali㉿kali)-[~/Documents/NT140/Lab02]
$ host noexist.uit.edu.vn
noexist.uit.edu.vn has address 45.122.249.78
noexist.uit.edu.vn has address 118.69.123.140

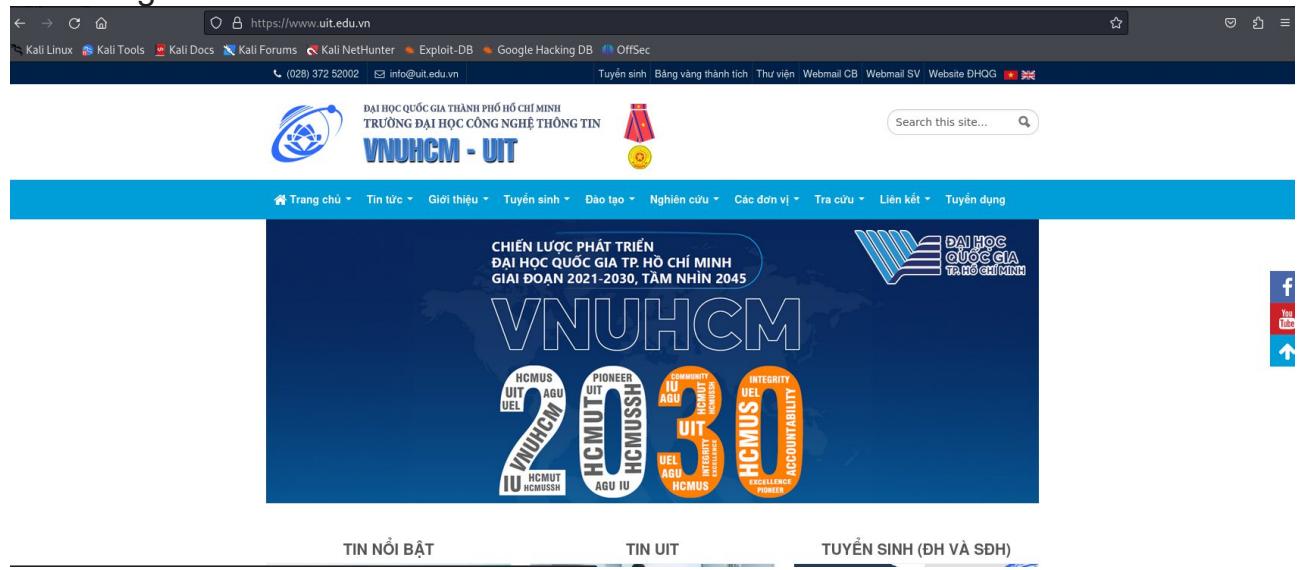
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ host baithuchanhso2.uit.edu.vn
baithuchanhso2.uit.edu.vn has address 45.122.249.78
baithuchanhso2.uit.edu.vn has address 118.69.123.140
```

Lí do hostname không tồn tại mà vẫn trả về địa chỉ ip là vì bản ghi dns đại diện (Wildcard DNS record) được sử dụng.

Cách hoạt động của bản ghi này:

Bản ghi thường được người quản lý tên miền sử dụng để đảm bảo những tên miền phụ không tồn tại hoặc không được sử dụng vẫn được xử lý đến máy chủ mặc định.

Thường địa chỉ này sẽ dẫn đến một trang báo lỗi hoặc trong trường hợp này đưa đến trang chính của tên miền uit.edu.vn:



### Forward Lookup Brute Force

```
(root㉿kali)-[~/home/kali/Desktop]
# cat list.txt
www
ftp
mail
owa
proxy
router
admin
www2
firewall
mx
pop3
dns
ca
```

```
(root㉿kali)-[~/home/kali/Desktop]
# for ip in $(cat list.txt); do host $ip.megacorpone.com; done
www.megacorpone.com has address 149.56.244.87
Host ftp.megacorpone.com not found: 3(NXDOMAIN)
mail.megacorpone.com has address 167.114.21.68
Host owa.megacorpone.com not found: 3(NXDOMAIN)
Host proxy.megacorpone.com not found: 3(NXDOMAIN)
router.megacorpone.com has address 167.114.21.70
admin.megacorpone.com has address 167.114.21.64
www2.megacorpone.com has address 149.56.244.87
Host firewall.megacorpone.com not found: 3(NXDOMAIN)
Host mx.megacorpone.com not found: 3(NXDOMAIN)
Host pop3.megacorpone.com not found: 3(NXDOMAIN)
Host dns.megacorpone.com not found: 3(NXDOMAIN)
Host ca.megacorpone.com not found: 3(NXDOMAIN)
```

#### ④ Bài tập về nhà (Yêu cầu làm)

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

Để sử dụng worklist rockyou, chỉ cần thay đổi phần list.txt bằng đường dẫn của tệp rockyou.txt

Với rockyou thì không tìm thấy hostname

## Lab 02: Information Gathering

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
└─$ for ip in $(cat /usr/share/wordlists/rockyou.txt); do host $ip.megacorpone.com; done
[1] + suspended host $ip.megacorpone.com
Host 123456.megacorpone.com not found: 3(NXDOMAIN)
Host 12345.megacorpone.com not found: 3(NXDOMAIN)
Host 123456789.megacorpone.com not found: 3(NXDOMAIN)
Host password.megacorpone.com not found: 3(NXDOMAIN)
Host iloveyou.megacorpone.com not found: 3(NXDOMAIN)
Host princess.megacorpone.com not found: 3(NXDOMAIN)
Host 1234567.megacorpone.com not found: 3(NXDOMAIN)
Host rockyou.megacorpone.com not found: 3(NXDOMAIN)
Host 12345678.megacorpone.com not found: 3(NXDOMAIN)
Host abc123.megacorpone.com not found: 3(NXDOMAIN)
Host nicole.megacorpone.com not found: 3(NXDOMAIN)
Host daniel.megacorpone.com not found: 3(NXDOMAIN)
Host babygirl.megacorpone.com not found: 3(NXDOMAIN)
Host monkey.megacorpone.com not found: 3(NXDOMAIN)
Host lovely.megacorpone.com not found: 3(NXDOMAIN)
Host jessica.megacorpone.com not found: 3(NXDOMAIN)
Host 654321.megacorpone.com not found: 3(NXDOMAIN)
Host michael.megacorpone.com not found: 3(NXDOMAIN)
Host ashley.megacorpone.com not found: 3(NXDOMAIN)
Host qwerty.megacorpone.com not found: 3(NXDOMAIN)
Host 111111.megacorpone.com not found: 3(NXDOMAIN)
Host iloveu.megacorpone.com not found: 3(NXDOMAIN)
Host 000000.megacorpone.com not found: 3(NXDOMAIN)
Host michelle.megacorpone.com not found: 3(NXDOMAIN)
Host tigger.megacorpone.com not found: 3(NXDOMAIN)
Host sunshine.megacorpone.com not found: 3(NXDOMAIN)
Host chocolate.megacorpone.com not found: 3(NXDOMAIN)
Host password1.megacorpone.com not found: 3(NXDOMAIN)
Host soccer.megacorpone.com not found: 3(NXDOMAIN)
```

Tương tự với Seclist thì thay bằng đường dẫn đến tệp đó  
 Ví dụ ở đây sử dụng tệp subdomains-top1million-5000.txt  
 Sau khi chạy một thời gian sau thì chỉ có những hostname sau tìm được ip

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
└─$ for ip in $(cat /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt); do host $ip.megacorpone.com; done
www.megacorpone.com has address 149.56.244.87
mail.megacorpone.com has address 167.114.21.68
Host ftp.megacorpone.com not found: 3(NXDOMAIN)
Host localhost.megacorpone.com not found: 3(NXDOMAIN)
Host webmail.megacorpone.com not found: 3(NXDOMAIN)
Host smtp.megacorpone.com not found: 3(NXDOMAIN)
Host webdisk.megacorpone.com not found: 3(NXDOMAIN)
Host pop.megacorpone.com not found: 3(NXDOMAIN)
Host cpanel.megacorpone.com not found: 3(NXDOMAIN)
Host whm.megacorpone.com not found: 3(NXDOMAIN)
ns1.megacorpone.com has address 51.79.37.18
ns2.megacorpone.com has address 51.222.39.63
Host autodiscover.megacorpone.com not found: 3(NXDOMAIN)
Host autoconfig.megacorpone.com not found: 3(NXDOMAIN)
Host ns.megacorpone.com not found: 3(NXDOMAIN)
test.megacorpone.com has address 167.114.21.75
Host m.megacorpone.com not found: 3(NXDOMAIN)
Host blog.megacorpone.com not found: 3(NXDOMAIN)
Host dev.megacorpone.com not found: 3(NXDOMAIN)
www2.megacorpone.com has address 149.56.244.87
ns3.megacorpone.com has address 66.70.207.180
Host pop3.megacorpone.com not found: 3(NXDOMAIN)
Host forum.megacorpone.com not found: 3(NXDOMAIN)
admin.megacorpone.com has address 167.114.21.64
mail2.megacorpone.com has address 167.114.21.69
vpn.megacorpone.com has address 167.114.21.76
Host mx.megacorpone.com not found: 3(NXDOMAIN)
Host imap.megacorpone.com not found: 3(NXDOMAIN)
Host old.megacorpone.com not found: 3(NXDOMAIN)
Host new.megacorpone.com not found: 3(NXDOMAIN)
```

### Reverse Lookup Brute Force

## Lab 02: Information Gathering

```
(root@kali)-[/home/kali/Desktop]
# for ip in $(seq 50 100); do host 38.100.193.$ip;done | grep -v "not found"
69.193.100.38.in-addr.arpa domain name pointer beta.megacorpone.com.
70.193.100.38.in-addr.arpa domain name pointer ns1.megacorpone.com.
72.193.100.38.in-addr.arpa domain name pointer admin.megacorpone.com.
73.193.100.38.in-addr.arpa domain name pointer mail2.megacorpone.com.
76.193.100.38.in-addr.arpa domain name pointer www.megacorpone.com.
77.193.100.38.in-addr.arpa domain name pointer vpn.megacorpone.com.
80.193.100.38.in-addr.arpa domain name pointer ns2.megacorpone.com.
85.193.100.38.in-addr.arpa domain name pointer snmp.megacorpone.com.
89.193.100.38.in-addr.arpa domain name pointer siem.megacorpone.com.
90.193.100.38.in-addr.arpa domain name pointer ns3.megacorpone.com.
91.193.100.38.in-addr.arpa domain name pointer router.megacorpone.com.
```

### DNS Zone Transfers

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ host -l megacorpone.com ns1.megacorpone.com
Using domain server:
Name: ns1.megacorpone.com
Address: 51.79.37.18#53
Aliases:

Host megacorpone.com not found: 5(REFUSED)
; Transfer failed.
```

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ host -l megacorpone.com ns2.megacorpone.com
Using domain server:
Name: ns2.megacorpone.com
Address: 51.222.39.63#53
Aliases:

megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
megacorpone.com name server ns3.megacorpone.com.
admin.megacorpone.com has address 167.114.21.64
beta.megacorpone.com has address 167.114.21.65
fs1.megacorpone.com has address 167.114.21.66
intranet.megacorpone.com has address 167.114.21.67
mail.megacorpone.com has address 167.114.21.68
mail2.megacorpone.com has address 167.114.21.69
ns1.megacorpone.com has address 51.79.37.18
ns2.megacorpone.com has address 51.222.39.63
ns3.megacorpone.com has address 66.70.207.180
router.megacorpone.com has address 167.114.21.70
siem.megacorpone.com has address 167.114.21.71
snmp.megacorpone.com has address 167.114.21.72
support.megacorpone.com has address 167.114.21.74
syslog.megacorpone.com has address 167.114.21.73
test.megacorpone.com has address 167.114.21.75
vpn.megacorpone.com has address 167.114.21.76
vpn2.megacorpone.com has address 167.114.21.77
vpndev.megacorpone.com has address 167.114.21.78
vpnprod.megacorpone.com has address 167.114.21.79
www.megacorpone.com has address 149.56.244.87
www2.megacorpone.com has address 149.56.244.87
```

#### Bài tập về nhà (Yêu cầu làm)

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](http://hcmus.edu.vn), [hcmussh.edu.vn](http://hcmussh.edu.vn), [uit.edu.vn](http://uit.edu.vn), [hcmut.edu.vn](http://hcmut.edu.vn), [hcmiu.edu.vn](http://hcmiu.edu.vn), [uel.edu.vn](http://uel.edu.vn), [hcmier.edu.vn](http://hcmier.edu.vn), [vnuhcm.edu.vn](http://vnuhcm.edu.vn)) và thực hiện zone transfer ứng với các nameserver đã tìm được.

Để thực hiện được có thể sử dụng Dig cho việc dễ dàng hơn khi tìm tên miền con  
Sử dụng đoạn code sau để thực hiện

```
#!/bin/bash
```

```
# Danh sách domain của các đơn vị thành viên
domains=("hcmus.edu.vn" "hcmussh.edu.vn" "uit.edu.vn" "hcmut.edu.vn"
"hcmiu.edu.vn" "uel.edu.vn" "hcmier.edu.vn" "vnuhcm.edu.vn")

# Hàm thực hiện tìm nameserver và zone transfer
perform_zone_transfer() {
    domain=$1
    echo "==== Domain: $domain ==="

    # Tìm các nameserver cho domain
    nameservers=$(dig NS $domain +short)

    if [ -z "$nameservers" ]; then
        echo "Không tìm thấy nameserver nào cho $domain"
        return
    fi

    echo "Nameserver cho $domain:"
    echo "$nameservers"

    # Thử zone transfer trên từng nameserver
    for ns in $nameservers; do
        echo "Thử zone transfer từ $ns"
        dig AXFR $domain @$ns

        done
        echo ""
    done
}

# Lặp qua từng domain trong danh sách
for domain in "${domains[@]}"; do
    perform_zone_transfer $domain
done
```

Kết quả sau khi thực hiện:



```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ ./zone_transfer.sh
==== Domain: hcmus.edu.vn ====
Nameserver cho hcmus.edu.vn:
server.hcmus.edu.vn.
dns2.hcmus.edu.vn.

Thử zone transfer từ server.hcmus.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmus.edu.vn @server.hcmus.edu.vn.
;; global options: +cmd
; Transfer failed.

Thử zone transfer từ dns2.hcmus.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmus.edu.vn @dns2.hcmus.edu.vn.
;; global options: +cmd
hcmus.edu.vn.      1800     IN      SOA      server.hcmus.edu.vn. netadmin.hcmus.edu.vn. 2024103025 600 300 3600 900
; Transfer failed.
```

## Lab 02: Information Gathering

```
== Domain: hcmussh.edu.vn ==
Nameserver cho hcmussh.edu.vn:
ns1.vdconline.vn.
ns2.vdconline.vn.
Thứ zone transfer từ ns1.vdconline.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmussh.edu.vn @ns1.vdconline.vn.
;; global options: +cmd
; Transfer failed.
Thứ zone transfer từ ns2.vdconline.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmussh.edu.vn @ns2.vdconline.vn.
;; global options: +cmd
; Transfer failed.
```

```
== Domain: uit.edu.vn ==
Nameserver cho uit.edu.vn:
nsbak.pavietnam.net.
ns1.pavietnam.vn.
ns2.pavietnam.vn.
Thứ zone transfer từ nsbak.pavietnam.net.

; <>> DiG 9.20.0-Debian <>> AXFR uit.edu.vn @nsbak.pavietnam.net.
;; global options: +cmd
; Transfer failed.
Thứ zone transfer từ ns1.pavietnam.vn.

; <>> DiG 9.20.0-Debian <>> AXFR uit.edu.vn @ns1.pavietnam.vn.
;; global options: +cmd
; Transfer failed.
Thứ zone transfer từ ns2.pavietnam.vn.

; <>> DiG 9.20.0-Debian <>> AXFR uit.edu.vn @ns2.pavietnam.vn.
;; global options: +cmd
; Transfer failed.
```

```
== Domain: hcmut.edu.vn ==
Nameserver cho hcmut.edu.vn:
dns3.hcmut.edu.vn.
dns1.hcmut.edu.vn.
dns4.hcmut.edu.vn.
dns2.hcmut.edu.vn.
Thứ zone transfer từ dns3.hcmut.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmut.edu.vn @dns3.hcmut.edu.vn.
;; global options: +cmd
; Transfer failed.
Thứ zone transfer từ dns1.hcmut.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmut.edu.vn @dns1.hcmut.edu.vn.
;; global options: +cmd
; Transfer failed.
Thứ zone transfer từ dns4.hcmut.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmut.edu.vn @dns4.hcmut.edu.vn.
;; global options: +cmd
; Transfer failed.
Thứ zone transfer từ dns2.hcmut.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmut.edu.vn @dns2.hcmut.edu.vn.
;; global options: +cmd
; Transfer failed.
```

```
== Domain: hcmiu.edu.vn ==
Nameserver cho hcmiu.edu.vn:
vdc-hn01.vnn.vn.
hcm-server1.vnn.vn.
Thứ zone transfer từ vdc-hn01.vnn.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmiu.edu.vn @vdc-hn01.vnn.vn.
;; global options: +cmd
; Transfer failed.
Thứ zone transfer từ hcm-server1.vnn.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmiu.edu.vn @hcm-server1.vnn.vn.
;; global options: +cmd
; Transfer failed.
```

**Lab 02: Information Gathering**

```
== Domain: uel.edu.vn ==
Nameserver cho uel.edu.vn:
ns2.dns.net.vn.
ns1.dns.net.vn.
Thử zone transfer từ ns2.dns.net.vn.

; <>> DiG 9.20.0-Debian <>> AXFR uel.edu.vn @ns2.dns.net.vn.
;; global options: +cmd
; Transfer failed.
Thử zone transfer từ ns1.dns.net.vn.

; <>> DiG 9.20.0-Debian <>> AXFR uel.edu.vn @ns1.dns.net.vn.
;; global options: +cmd
; Transfer failed.
```

```
== Domain: hcmier.edu.vn ==
Nameserver cho hcmier.edu.vn:
server.vnuhcm.edu.vn.
vnuserv.vnuhcm.edu.vn.
Thử zone transfer từ server.vnuhcm.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmier.edu.vn @server.vnuhcm.edu.vn.
;; global options: +cmd
; Transfer failed.
Thử zone transfer từ vnuserv.vnuhcm.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR hcmier.edu.vn @vnuserv.vnuhcm.edu.vn.
;; global options: +cmd
; Transfer failed.
```

```
== Domain: vnuhcm.edu.vn ==
Nameserver cho vnuhcm.edu.vn:
vnuserv.vnuhcm.edu.vn.
ns2.vdc2.vn.
ns1.vdc2.vn.
server.vnuhcm.edu.vn.
Thử zone transfer từ vnuserv.vnuhcm.edu.vn.

; <>> DiG 9.20.0-Debian <>> AXFR vnuhcm.edu.vn @vnuserv.vnuhcm.edu.vn.
;; global options: +cmd
; Transfer failed.
Thử zone transfer từ ns2.vdc2.vn.

; <>> DiG 9.20.0-Debian <>> AXFR vnuhcm.edu.vn @ns2.vdc2.vn.
;; global options: +cmd
vnuhcm.edu.vn.    60    IN    SOA    vnuserv.vnuhcm.edu.vn. info.vdc2.vn. 2023080147 3 1 604800 10800
vnuhcm.edu.vn.    60    IN    NS     vnuserv.vnuhcm.edu.vn.
vnuhcm.edu.vn.    60    IN    NS     server.vnuhcm.edu.vn.
vnuhcm.edu.vn.    60    IN    A      103.88.121.29
vnuhcm.edu.vn.    60    IN    MX    10 aspmx.l.google.com.
vnuhcm.edu.vn.    60    IN    MX    20 alt1.aspmx.l.google.com.
vnuhcm.edu.vn.    60    IN    MX    25 alt2.aspmx.l.google.com.
vnuhcm.edu.vn.    60    IN    MX    30 aspmx2.googlemail.com.
vnuhcm.edu.vn.    60    IN    MX    40 aspmx4.googlemail.com.
vnuhcm.edu.vn.    60    IN    MX    45 aspmx5.googlemail.com.
vnuhcm.edu.vn.    60    IN    TXT   "v=spf1 ip4:103.88.121.53/32 include:_spf.google.com ~all"
www.4s.vnuhcm.edu.vn. 60    IN    A      118.69.204.199
default._domainkey.vnuhcm.edu.vn. 60 IN CNAME mailpro.mailserver.vn.
mail._domainkey.vnuhcm.edu.vn. 60 IN TXT "v=DKIM1; h=sha256; k=rsa; s=email; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDzwt7Y3SQ7Jm5rwr8DvXM2VQ4Xoxu6s28C5p4t3MVsAu4q4tOhRuUm7idAykpoo3tKAhovoXOWDug9+jr2*x465/YpGoq1ueJNrp0Imc8rX8k96KO6x/8FxSchvdq0FDePI8VapKKQNEUq9zgtGaNx7gm/ax0vQ Ae9wmSBMmwIDAQAB"
aaa.vnuhcm.edu.vn.    60    IN    A      103.88.123.21
```

**DNSRecon**

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ dnsrecon -d megacorpone.com -t axfr
[*] Checking for Zone Transfer for megacorpone.com name servers
[*] Resolving megacorpone.com
[*] Resolving NS ns1.megacorpone.com 51.79.37.18
[*] Resolving NS Records
[*] NS Servers found:
[*]   NS ns2.megacorpone.com 51.222.39.63
[*]   NS ns1.megacorpone.com 51.79.37.18
[*]   NS ns3.megacorpone.com 66.70.207.180
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 51.79.37.18
[*] 51.79.37.18 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 66.70.207.180
[*] 66.70.207.180 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 51.222.39.63
[*] 51.222.39.63 Has port 53 TCP Open
[*] Zone Transfer was successful!!
[*] SOA ns1 125.235.4.59
[*] NS ns1.megacorpone.com 51.79.37.18
[*] NS ns2.megacorpone.com 51.222.39.63
[*] NS ns3.megacorpone.com 66.70.207.180
[*] TXT Try Harder
[*] TXT google-site-verification-UTB_b0HNeBy4qYGQZNsEYXFJCJ2hMNV3GtC0wWq5pA
[*] MX @.megacorpone.com fb.mail.gandi.net 217.70.178.217
[*] MX @.megacorpone.com fb.mail.gandi.net 217.70.178.216
[*] MX @.megacorpone.com fb.mail.gandi.net 2001:4b98:dc4:8::217
[*] MX @.megacorpone.com fb.mail.gandi.net 2001:4b98:dc4:8::215
[*] MX @.megacorpone.com fb.mail.gandi.net 2001:4b98:dc4:8::216
[*] MX @.megacorpone.com spool.mail.gandi.net 217.70.178.1
[*] MX @.megacorpone.com spool.mail.gandi.net 2001:4b98:e00::1
[*] MX @.megacorpone.com mail 125.235.4.59
[*] MX @.megacorpone.com mail 167.114.21.64
[*] A admin.megacorpone.com 167.114.21.64
[*] A beta.megacorpone.com 167.114.21.65
[*] A fsl.megacorpone.com 167.114.21.66
[*] A intranet.megacorpone.com 167.114.21.67
[*] A mail.megacorpone.com 167.114.21.68
[*] A mail2.megacorpone.com 167.114.21.69
```

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ cat list.txt
www
ftp
mail
owa
proxy
router
admin
www2
firewall
mx
pop3
dns
ca

(kali㉿kali)-[~/Documents/NT140/Lab02]
$ dnsrecon -d megacorpone.com -D list.txt -t brt
[*] Using the dictionary file: list.txt (provided by user)
[*] brt: Performing host and subdomain brute force against megacorpone.com...
[!]Wildcard resolution is enabled on this domain
[!] It is resolving to 125.235.4.59
[!] All queries will resolve to this list of addresses!!
[*] Do you wish to continue? [Y/n]
y
[+] A ftp.megacorpone.com 125.235.4.59
[+] A www.megacorpone.com 149.56.244.87
[+] A mail.megacorpone.com 167.114.21.68
[+] A proxy.megacorpone.com 125.235.4.59
[+] A owa.megacorpone.com 125.235.4.59
[+] A www2.megacorpone.com 149.56.244.87
[+] A admin.megacorpone.com 167.114.21.64
[+] A router.megacorpone.com 167.114.21.70
[+] A firewall.megacorpone.com 125.235.4.59
[+] A pop3.megacorpone.com 125.235.4.59
[+] A mx.megacorpone.com 125.235.4.59
[+] A ca.megacorpone.com 125.235.4.59
[+] A dns.megacorpone.com 125.235.4.59
[+] 13 Records Found
```

### ④ Bài tập về nhà (Cộng điểm)

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

-t

- std(Standard Enumeration): Thực hiện truy vấn thông thường các bản ghi: SOA, NS, A, AAAA, MX and SRV.

-brt(Brute Force Subdomain): Thực hiện brute force subdomain và host sử dụng từ điển(dictionary)

-srv(SRV Records Enumeration): Truy vấn các bản ghi SRV

-axfr(Test for Zone Transfers): Kiểm tra khả năng zone transfer bằng cách sử dụng các truy vấn AXFR tới các nameserver.

-rvl(Reverse Lookup of a Given CIDR Range): Thực hiện reverse lookup trên một dải IP (CIDR) để tìm các bản ghi PTR liên kết với các IP đó.

-bing: Sử dụng công cụ tìm kiếm bing để tìm host và tên miền

-yand: Sử dụng công cụ tìm kiếm yand để tìm host và tên miền

-crt: Sử dụng crt.sh để liệt kê qua nhầm tìm host và tên miền con.

-snoop: Lưu đói số snooping vào máy chủ NS

-tld: Kiểm tra các TLD được IANA ký

- zonewalk: Thực hiện “zone walking” để tìm danh sách các bản ghi trong một zone được DNSSEC ký.

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

Ví dụ: Thực hiện Standard Enumeration và kiểm tra Zone Transfer  
 dnsrecon -d example.com -t std,axfr

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ dnsrecon -d megacorpone.com -t std,axfr
[*] Checking for Zone Transfer for megacorpone.com name servers
[*] Resolving SOA Record
[*]      SOA ns1.megacorpone.com 51.79.37.18
[*] Resolving NS Records
[*] NS Servers found:
[*]      NS ns3.megacorpone.com 66.70.207.180
[*]      NS ns1.megacorpone.com 51.79.37.18
[*]      NS ns2.megacorpone.com 51.222.39.63
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 51.79.37.18
[-] Zone Transfer Failed for 51.79.37.18!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 51.222.39.63
[-] Zone Transfer Failed for 51.222.39.63!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 66.70.207.180
[-] Zone Transfer Failed for 66.70.207.180!
[-] Port 53 TCP is being filtered
[*] std: Performing General Enumeration against: megacorpone.com ...
[*] Wildcard resolution is enabled on this domain
[*] It is resolving to 125.235.4.59
[*] All queries will resolve to this list of addresses !!
[-] DNSSEC is not configured for megacorpone.com
[*]      SOA ns1.megacorpone.com 51.79.37.18
[*]      NS ns3.megacorpone.com 66.70.207.180
```

Thực hiện Brute Force Subdomain và kiểm tra Reverse Lookup  
 dnsrecon -d example.com -t brt,rvl

**Lab 02: Information Gathering**

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ dnsrecon -d megacorpone.com -t brt,rvl
[*] No dictionary file has been specified.
[*] Using the dictionary file: /usr/share/dnsrecon/dnsrecon/data/namelist.txt (provided by tool)
[*] brt: Performing host and subdomain brute force against megacorpone.com ...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 125.235.4.59
[!] All queries will resolve to this list of addresses !!
[*] Do you wish to continue? [Y/n]
y
[+] A 03.megacorpone.com 125.235.4.59
[+] A 12.megacorpone.com 125.235.4.59
[+] A 11.megacorpone.com 125.235.4.59
[+] A 0.megacorpone.com 125.235.4.59
[+] A 1.megacorpone.com 125.235.4.59
[+] A 10.megacorpone.com 125.235.4.59
[+] A 01.megacorpone.com 125.235.4.59
[+] A 02.megacorpone.com 125.235.4.59
[+] A 14.megacorpone.com 125.235.4.59
[+] A 13.megacorpone.com 125.235.4.59
[+] A 16.megacorpone.com 125.235.4.59
[+] A 19.megacorpone.com 125.235.4.59
[+] A 2.megacorpone.com 125.235.4.59
[+] A 15.megacorpone.com 125.235.4.59
[+] A 17.megacorpone.com 125.235.4.59
[+] A 3.megacorpone.com 125.235.4.59
[+] A 20.megacorpone.com 125.235.4.59
[+] A 3com.megacorpone.com 125.235.4.59
[+] A 5.megacorpone.com 125.235.4.59
[+] A 4.megacorpone.com 125.235.4.59
[+] A 6.megacorpone.com 125.235.4.59
[+] A 7.megacorpone.com 125.235.4.59
```

**DNSEnum**

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ dnsenum megacorpone.com
dnsenum VERSION:1.3.1

megacorpone.com
list.txt    output.txt    zone_transfer.sh

Host's addresses:
aylavmaasmdo.megacorpone.com.      5      IN      A      125.235.4.59
!!!!!!!!

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

Name Servers:
ns1.megacorpone.com.      5      IN      A      51.79.37.18
ns2.megacorpone.com.      5      IN      A      51.222.39.63
ns3.megacorpone.com.      5      IN      A      66.70.207.180

Mail (MX) Servers:
spool.mail.gandi.net.      5      IN      A      217.70.178.1
mail.megacorpone.com.      5      IN      A      167.114.21.68
mail2.megacorpone.com.      5      IN      A      167.114.21.69
fb.mail.gandi.net.      5      IN      A      217.70.178.215
fb.mail.gandi.net.      5      IN      A      217.70.178.217
fb.mail.gandi.net.      5      IN      A      217.70.178.216
```

## ⑧ Bài tập về nhà (Cộng điểm)

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?

	DNSEnum	DNSRecon
Tính năng	<ul style="list-style-type: none"> <li>-Thực hiện brute force subdomain.</li> <li>-Tìm các bản ghi DNS cơ bản như A, AAAA, MX, NS.</li> <li>Kiểm tra zone transfer (AXFR).</li> <li>-Truy xuất các bản ghi whois, PTR.</li> <li>-Hỗ trợ các file danh sách từ để brute force subdomain.</li> </ul>	<ul style="list-style-type: none"> <li>-Hỗ trợ nhiều loại truy vấn DNS (A, AAAA, MX, NS, SOA, SRV, TXT, CNAME).</li> <li>-Tích hợp các tùy chọn brute force subdomain và reverse lookup.</li> <li>-Kiểm tra khả năng zone transfer.</li> <li>-Hỗ trợ enumeration qua DNSSEC với tùy chọn zonewalk.</li> <li>-Hỗ trợ tìm kiếm subdomain qua Bing.</li> <li>-Hỗ trợ kiểm tra DNS dựa trên dải CIDR.</li> </ul>
Ưu điểm	<ul style="list-style-type: none"> <li>-Dễ sử dụng với các tùy chọn cơ bản.</li> <li>-Thích hợp cho các tác vụ DNS enumeration đơn giản.</li> </ul>	<ul style="list-style-type: none"> <li>-Cung cấp nhiều tùy chọn và tính năng nâng cao.</li> <li>-Linh hoạt hơn DNSEnum với khả năng tùy chỉnh chi tiết các tùy chọn.</li> <li>-Hỗ trợ kiểm tra DNSSEC và nhiều loại bản ghi hơn</li> </ul>
Nhược điểm	<ul style="list-style-type: none"> <li>-Hạn chế về tính năng nâng cao, ít tùy chọn</li> </ul>	<ul style="list-style-type: none"> <li>-Không thích hợp với người dùng mới</li> </ul>

Công cụ nào dễ sử dụng hơn: Dnsenum

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

## K. Port Scanning

### Stealth/SYN Scanning

## Lab 02: Information Gathering

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ sudo nmap -sS 192.168.108.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 14:49 +07
Nmap scan report for 192.168.108.128
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```

### ⑧ Bài tập về nhà (Yêu cầu làm)

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

Mở wireshark rồi chạy lại câu lệnh: sudo nmap -sS <ip của Metasploitable 2>

Sau khi chạy thì thấy rằng, ví dụ như gói tin thứ 11 :

Gửi yêu cầu SYN từ cổng 43280 đến cổng 554: Đây là máy khách gửi yêu cầu SYN đến máy chủ.

Ở gói tin 22: Gửi đáp lại RST,ACK từ cổng 554 đến 43280: Đây là máy chủ đáp lại máy khách RST(reset), ACK(acknowledgment) nghĩa là kết nối không chấp nhận (cổng không mở cho kết nối)

11	13.103659342	192.168.108.130	192.168.108.128	TCP	58 43280 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	13.103713967	192.168.108.130	192.168.108.128	TCP	58 43280 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	13.103740392	192.168.108.130	192.168.108.128	TCP	58 43280 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	13.103761539	192.168.108.130	192.168.108.128	TCP	58 43280 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	13.103792329	192.168.108.130	192.168.108.128	TCP	58 43280 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	13.103812927	192.168.108.130	192.168.108.128	TCP	58 43280 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	13.103844051	192.168.108.130	192.168.108.128	TCP	58 43280 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	13.103875652	192.168.108.130	192.168.108.128	TCP	58 43280 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	13.103900293	192.168.108.130	192.168.108.128	TCP	58 43280 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	13.103935757	192.168.108.130	192.168.108.128	TCP	58 43280 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	13.103936168	192.168.108.128	192.168.108.130	TCP	60 554 → 43280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	13.103936386	192.168.108.128	192.168.108.130	TCP	60 1025 → 43280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	13.105661908	192.168.108.128	192.168.108.130	TCP	60 23 → 43280 [SYN, ACK] Seq=0 Ack=1 Win=5640 Len=0 MSS=1460

Một ví dụ khác nếu cổng mở thì:

Ở gói tin 13 yêu cầu kết nối đến cổng 23

Ở gói tin 23 thì máy chủ đáp lại với SYN,ACK nghĩa là cho phép kết nối, kết nối thành công

13	13.103740392	192.168.108.130	192.168.108.128	TCP	58 43280 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	13.103761539	192.168.108.130	192.168.108.128	TCP	58 43280 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	13.103792329	192.168.108.130	192.168.108.128	TCP	58 43280 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	13.103812927	192.168.108.130	192.168.108.128	TCP	58 43280 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	13.103844051	192.168.108.130	192.168.108.128	TCP	58 43280 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	13.103875652	192.168.108.130	192.168.108.128	TCP	58 43280 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	13.103900293	192.168.108.130	192.168.108.128	TCP	58 43280 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	13.103935757	192.168.108.130	192.168.108.128	TCP	58 43280 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	13.103936168	192.168.108.128	192.168.108.130	TCP	60 554 → 43280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	13.103936386	192.168.108.128	192.168.108.130	TCP	60 1025 → 43280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	13.105661908	192.168.108.128	192.168.108.130	TCP	60 23 → 43280 [SYN, ACK] Seq=0 Ack=1 Win=5640 Len=0 MSS=1460

**Lab 02: Information Gathering**

Sau khi đã kết nối và thực hiện những gì cần thiết, ở gói tin thứ 31 :  
Máy khách gửi yêu cầu RST từ cổng 43280 đến cổng 23 để yêu cầu đóng kết nối

23 13.105061908	192.168.108.128	192.168.108.130	TCP	60 23 → 43280 [SYN, ACK] Seq=0 Ack=1 Win=0 MSS=1460
24 13.105062108	192.168.108.128	192.168.108.130	TCP	60 110 → 43280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25 13.105062157	192.168.108.128	192.168.108.130	TCP	60 111 → 43280 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
26 13.105062201	192.168.108.128	192.168.108.130	TCP	60 5900 → 43280 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
27 13.105062246	192.168.108.128	192.168.108.130	TCP	60 139 → 43280 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
28 13.105062291	192.168.108.128	192.168.108.130	TCP	60 25 → 43280 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
29 13.105062337	192.168.108.128	192.168.108.130	TCP	60 1723 → 43280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30 13.105062381	192.168.108.128	192.168.108.130	TCP	60 587 → 43280 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31 13.105114226	192.168.108.130	192.168.108.128	TCP	54 43280 → 23 [RST] Seq=1 Win=0 Len=0

**TCP Connect Scanning**

```
└ $ sudo nmap -sT 192.168.108.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 14:58 +07
Nmap scan report for 192.168.108.128
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:8B:D0:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

**④ Bài tập về nhà (Yêu cầu làm)**

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

Tương tự mở wiredshark và chạy lại lệnh : sudo nmap -sT <ip> của Metasploitable  
2>

Cũng như trên thì cũng có 2 trường hợp

TH 1: Cổng đóng

Máy khách gửi SYN ở gói 23 đến cổng 993 : Yêu cầu kết nối 993

Máy chủ gửi RST,ACK ở gói 24: Từ chối kết nối

23 13.345643892	192.168.108.130	192.168.108.128	TCP	74 40706 → 993 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873907 TSectr=0 WS=128
24 13.346032592	192.168.108.128	192.168.108.130	TCP	60 993 → 40706 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

TH 2: Cổng mở

Ở đây là đến cổng 25

26 13.346252726	192.168.108.130	192.168.108.128	TCP	74 50040 → 25 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873908 TSectr=0 WS=128
27 13.346423307	192.168.108.130	192.168.108.128	TCP	74 36132 → 554 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873908 TSectr=0 WS=128
28 13.346507141	192.168.108.128	192.168.108.130	TCP	60 256 → 33258 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 13.346507430	192.168.108.128	192.168.108.130	TCP	74 25 → 50040 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TStamp=84506 TSecr=2645873908 WS=128
30 13.346516511	192.168.108.130	192.168.108.128	TCP	74 53140 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873908 TSectr=0 WS=128
31 13.346506355	192.168.108.130	192.168.108.128	TCP	66 50040 → 25 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=2645873908 TSectr=84506

Đầu tiên máy khách gửi SYN đến cổng 25 ở gói tin 26 : yêu cầu kết nối cổng 25

Máy chủ đáp lại với SYN, ACK ở gói 29 : Cho phép kết nối cổng 25

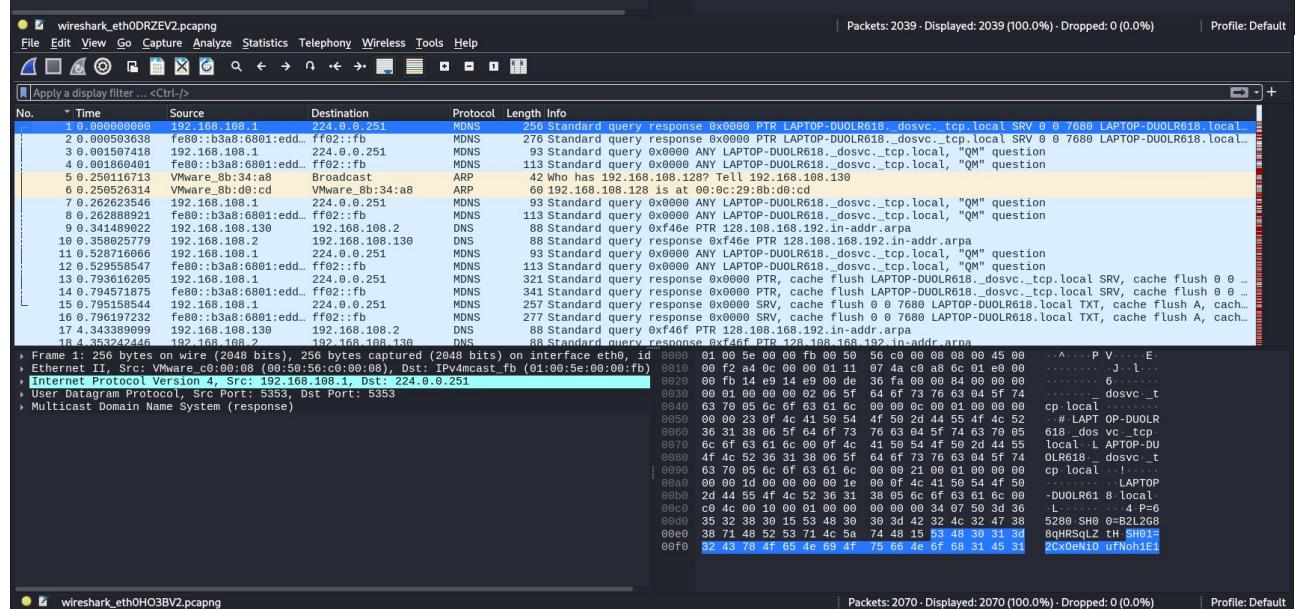
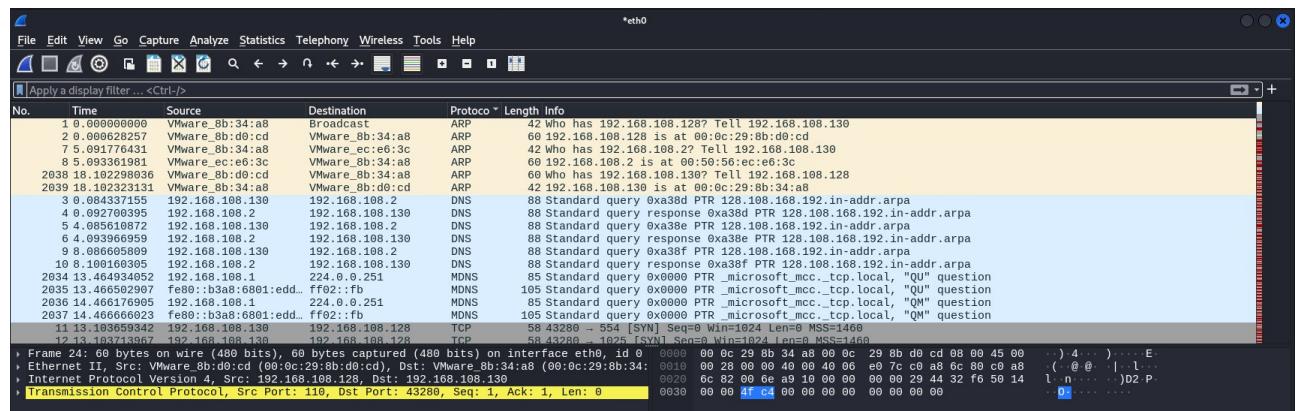
## Lab 02: Information Gathering

Máy khác đáp lại ACK ở gói 31: Cho máy chủ biết là đã nhận được thông tin và kết nối đến cổng 25

Sau khi thực hiện xong thì máy khách gửi RST,ACK để đóng kết nối ở gói 43

31 13. 346556355 192.168.108.130 192.168.108.128 TCP 66 50940 → 25 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=2645873908 TSectr=84506
32 13. 346755322 192.168.108.130 192.168.108.128 TCP 74 33546 → 8080 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873908 TSectr=0 WS=1
33 13. 346815331 192.168.108.128 192.168.108.130 TCP 60 554 → 36132 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34 13. 346815573 192.168.108.128 192.168.108.130 TCP 74 3369 → 53148 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TStamp=84506 TSectr=2
35 13. 346845364 192.168.108.130 192.168.108.128 TCP 74 59368 → 1025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873908 TSectr=0 WS=1
36 13. 346888879 192.168.108.130 192.168.108.128 TCP 66 53149 → 3396 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=2645873908 TSectr=84506
37 13. 346969354 192.168.108.130 192.168.108.128 TCP 74 53618 → 1723 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873908 TSectr=0 WS=1
38 13. 347072474 192.168.108.128 192.168.108.130 TCP 66 8980 → 33546 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39 13. 347072736 192.168.108.128 192.168.108.130 TCP 66 1025 → 59368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40 13. 347234518 192.168.108.128 192.168.108.130 TCP 66 1723 → 53618 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41 13. 347411584 192.168.108.130 192.168.108.128 TCP 74 47576 → 1720 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873908 TSectr=0 WS=1
42 13. 347554425 192.168.108.130 192.168.108.128 TCP 74 46380 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TStamp=2645873909 TSectr=0 WS=128
43 13. 347755744 192.168.108.130 192.168.108.128 TCP 66 50040 → 25 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TStamp=2645873909 TSectr=84506

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...)



	SYN Scan	TCP Connect Scan
Tổng số gói tin	2039	2070
Thời gian gửi/nhận	0.002	0.001
Số gói tin khi yêu cầu kết nối thành công	3	4

## UDP Scanning

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ sudo nmap --min-rate=1000 -sU 192.168.108.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:40 +07
Nmap scan report for 192.168.108.128
Host is up (0.00029s latency).
Not shown: 990 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
1901/udp  closed fjal-l-tep-a
2049/udp  open  nfs
2082/udp  closed unknown
20742/udp closed unknown
32779/udp closed sometimes-rpc22
49171/udp closed unknown
58419/udp closed unknown
MAC Address: 00:0C:29:8B:D0:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.32 seconds
```

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ sudo nmap --min-rate=1000 -sS -sU 192.168.108.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:36 +07
Nmap scan report for 192.168.108.128
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset), 10 closed udp ports (port-unreach), 986 open|filtered udp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
2049/udp  open  nfs
MAC Address: 00:0C:29:8B:D0:CD (VMware)

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:28 +07
Initiating ARP Ping Scan at 15:28
Scanning 192.168.108.128 [1 port]
Completed ARP Ping Scan at 15:28, @.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host, at 15:28
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, OR: 1, SF: 0, TR: 3, TQ: 1]
Initiating UDP Scan at 15:28
Scanning 192.168.108.128 [1000 ports]
Increasing send delay for 192.168.108.128 from 0 to 50 due to max_successful_tryno increase
Increasing send delay for 192.168.108.128 from 50 to 100 due to 11 out of 11 dropped probes
Increasing send delay for 192.168.108.128 from 100 to 200 due to 11 out of 12 dropped probes
UDP Scan Timing: About 9.55% done; ETC: 15:32 (0:04:54 remaining)
Increasing send delay for 192.168.108.128 from 200 to 400 due to 11 out of 15 dropped probes
Increasing send delay for 192.168.108.128 from 400 to 800 due to 11 out of 11 dropped probes
UDP Scan Timing: About 12.98% done; ETC: 15:34 (0:00:49 remaining)
Increasing send delay for 192.168.108.128 from 800 to 1000 due to 11 out of 19 dropped probes
UDP Scan Timing: About 14.95% done; ETC: 15:36 (0:00:38 remaining)
Increasing send delay for 192.168.108.128 from 1000 to 1200 due to 11 out of 12 dropped probes
UDP Scan Timing: About 17.95% done; ETC: 15:37 (0:00:13 remaining)
Discovered open port 53/udp on 192.168.108.128
UDP Scan Timing: About 40.45% done; ETC: 15:41 (0:00:38 remaining)

Nmap done: 1 IP address (1 host up) scanned in 17.69 seconds
```

## Network Sweeping

## Lab 02: Information Gathering

```
└─(kali㉿kali)-[~/Documents/NT140/Lab02]
$ sudo nmap --min-rate=1000 -sn 192.168.108.1-254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:46 +07
Nmap scan report for 192.168.108.1
Host is up (0.00076s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.108.2
Host is up (0.00028s latency).
MAC Address: 00:50:56:EC:E6:3C (VMware)
Nmap scan report for 192.168.108.128
Host is up (0.00028s latency).
MAC Address: 00:0C:29:88:D0:CD (VMware)
Nmap scan report for 192.168.108.254
Host is up (0.00019s latency).
MAC Address: 00:50:56:FD:09:0E (VMware)
Nmap scan report for 192.168.108.130
Host is up.
Nmap done: 254 IP addresses (5 hosts up) scanned in 26.77 seconds
```

```
└─(kali㉿kali)-[~/Documents/NT140/Lab02]
$ sudo nmap --min-rate=1000 -v -sn 192.168.108.1-254 -oG ping-sweep.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:47 +07
Initiating ARP Ping Scan at 15:47
Scanning 253 hosts [1 port/host]
Completed ARP Ping Scan at 15:47, 0.71s elapsed (253 total hosts)
Initiating Parallel DNS resolution of 4 hosts. at 15:47
Completed Parallel DNS resolution of 4 hosts. at 15:48, 13.00s elapsed
Nmap scan report for 192.168.108.1
Host is up (0.000088s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.108.2
Host is up (0.00018s latency).
MAC Address: 00:50:56:EC:E6:3C (VMware)
Nmap scan report for 192.168.108.3 [host down]
Nmap scan report for 192.168.108.4 [host down]
Nmap scan report for 192.168.108.5 [host down]
Nmap scan report for 192.168.108.6 [host down]
Nmap scan report for 192.168.108.7 [host down]
Nmap scan report for 192.168.108.8 [host down]
Nmap scan report for 192.168.108.9 [host down]
Nmap scan report for 192.168.108.10 [host down]
Nmap scan report for 192.168.108.11 [host down]
Nmap scan report for 192.168.108.12 [host down]
Nmap scan report for 192.168.108.13 [host down]
Nmap scan report for 192.168.108.14 [host down]
Nmap scan report for 192.168.108.15 [host down]
Nmap scan report for 192.168.108.16 [host down]
Nmap scan report for 192.168.108.17 [host down]
Nmap scan report for 192.168.108.18 [host down]
Nmap scan report for 192.168.108.19 [host down]
```

```
└─(kali㉿kali)-[~/Documents/NT140/Lab02]
$ grep Up ping-sweep.txt | cut -d " " -f 2
192.168.108.1
192.168.108.2
192.168.108.128
192.168.108.254
192.168.108.130
```

## Lab 02: Information Gathering

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
└─$ sudo nmap --min-rate=1000 -p 80 192.168.108.1-254 -oG web-sweep.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 15:50 +07
Nmap scan report for 192.168.108.1
Host is up (0.00042s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.108.2
Host is up (0.00019s latency).

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:50:56:EC:E6:3C (VMware)

Nmap scan report for 192.168.108.128
Host is up (0.00018s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:8B:D0:CD (VMware)

Nmap scan report for 192.168.108.254
Host is up (0.00021s latency).

PORT      STATE SERVICE
80/tcp    filtered http
MAC Address: 00:50:56:FD:09:0E (VMware)

Nmap scan report for 192.168.108.130
```

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
└─$ grep open web-sweep.txt | cut -d " " -f 2
192.168.108.1
192.168.108.128
```

### ④ Bài tập về nhà (Cộng điểm)

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

Câu lệnh thực hiện để ping là “ping -c 1 -W 1 192.168.108.1-254 > /dev/null 2>&1”  
Sau đây là lệnh đó được thực hiện trên 4 ngôn ngữ khác nhau:

Bash script:

```
1#!/bin/bash
2
3 network="192.168.108"
4
5 for ip in {1..254}; do
6   ping -c 1 -W 1 "$network.$ip" > /dev/null 2>&1
7   if [ $? -eq 0 ]; then
8     echo "Host $network.$ip is up"
9   fi
0 done
1
```

Kết quả:

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
└─$ ./ping.sh
Host 192.168.108.2 is up
Host 192.168.108.128 is up
Host 192.168.108.130 is up
```

Python:

```

1 import os
2
3 network = "192.168.108"
4 for ip in range(1, 255):
5     address = f"{network}.{ip}"
6     response = os.system(f"ping -c 1 -W 1 {address} > /dev/null 2>&1")
7     if response == 0:
8         print(f"Host {address} is up")
9
10

```

Kết quả:

```

└─(kali㉿kali)-[~/Documents/NT140/Lab02]
$ python3 pingpy.py
Host 192.168.108.2 is up
Host 192.168.108.128 is up
Host 192.168.108.130 is up

```

C:

```

1 #include <stdio.h>
2 #include <stdlib.h>
3
4 int main() {
5     char command[100];
6     char network[] = "192.168.108";
7
8     for (int i = 1; i <= 254; i++) {
9         sprintf(command, sizeof(command), "ping -c 1 -W 1 %s.%d > /dev/null 2>&1", network, i);
10        int response = system(command);
11        if (response == 0) {
12            printf("Host %s.%d is up\n", network, i);
13        }
14    }
15    return 0;
16 }

```

Kết quả:

```

└─(kali㉿kali)-[~/Documents/NT140/Lab02]
$ ./pingc
Host 192.168.108.2 is up
Host 192.168.108.128 is up
Host 192.168.108.130 is up

```

Perl:

```

#!/usr/bin/perl
my $network = "192.168.108";
for my $ip (1..254) {
    my $address = "$network.$ip";
    my $response = system("ping -c 1 -W 1 $address > /dev/null 2>&1");
    if ($response == 0) {
        print "Host $address is up\n";
    }
}

```

Kết quả:

```

└─(kali㉿kali)-[~/Documents/NT140/Lab02]
$ ./pingpl.pl
Host 192.168.108.2 is up
Host 192.168.108.128 is up
Host 192.168.108.130 is up

```

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

**Lab 02: Information Gathering**

Để phân tích, mở Wireshark và nhập câu lệnh sau:  
nmap --min-rate=1000 -sn 192.168.108.1-254

Khi thực hiện câu lệnh trên trong Wireshark sẽ thấy rất nhiều gói tin arp

Index	Source	Destination	Type	Length	Time	Content
2	0.0.0.0.121697	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.3? Tell 192.168.108.130	
3	0.0.0.0.232580	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.4? Tell 192.168.108.130	
4	0.0.0.0.315784	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.5? Tell 192.168.108.130	
5	0.0.0.0.394566	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.6? Tell 192.168.108.130	
6	0.0.0.0.474214	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.7? Tell 192.168.108.130	
7	0.0.0.0.552779	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.8? Tell 192.168.108.130	
8	0.0.0.0.638299	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.9? Tell 192.168.108.130	
9	0.0.0.0.698974	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.10? Tell 192.168.108.130	
10	0.0.0.0.790538	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.11? Tell 192.168.108.130	
11	0.0.0.0.1818883	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.12? Tell 192.168.108.130	
12	0.0.0.0.2815124	VMware_ec:e6:3c	Broadcast	ARP	60 Who has 192.168.108.13? Tell 192.168.108.2	
13	0.0.0.0.2834037	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.14? Tell 192.168.108.130	

Những gói tin này gửi đến địa chỉ broadcast để hỏi địa chỉ ip có thể kết nối đến thì nếu Wireshark bắt được gói này nghĩa là những địa chỉ này không thể kết nối  
Đối với các địa chỉ ip như:

**Địa chỉ .2**

Gửi gói tin SYN thành công

Nhưng địa chỉ đó đáp lại RST,ACK nghĩa là từ chối kết nối

Index	Source	Destination	Type	Length	Time	Content
1	0.0.0.0.0.0.0.0	192.168.108.130	192.168.108.2	TCP	74 49676 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=539627412 TSecr=0 WS=128	
2	0.0.0.0.121697	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.3? Tell 192.168.108.130	
3	0.0.0.0.232580	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.4? Tell 192.168.108.130	
4	0.0.0.0.315784	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.5? Tell 192.168.108.130	
5	0.0.0.0.394566	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.6? Tell 192.168.108.130	
6	0.0.0.0.474214	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.7? Tell 192.168.108.130	
7	0.0.0.0.552779	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.8? Tell 192.168.108.130	
8	0.0.0.0.638299	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.9? Tell 192.168.108.130	
9	0.0.0.0.698974	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.10? Tell 192.168.108.130	
10	0.0.0.0.790538	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.11? Tell 192.168.108.130	
11	0.0.0.0.1818883	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.12? Tell 192.168.108.130	
12	0.0.0.0.2815124	VMware_ec:e6:3c	Broadcast	ARP	60 Who has 192.168.108.13? Tell 192.168.108.2	
13	0.0.0.0.2834037	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.14? Tell 192.168.108.130	
14	0.0.0.0.2815389	192.168.108.2	192.168.108.130	TCP	60 89 - 49676 [RST, ACK] Seq=1 Ack=1 Win=32767 Len=0	

**Trong trường hợp địa chỉ .1**

Thay về từ chối như .2 thì gửi SYN, ACK nghĩa là chấp nhận kết nối

Index	Source	Destination	Type	Length	Time	Content
172	0.444285209	192.168.108.130	192.168.108.1	TCP	74 41896 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3240521692 TSecr=0 WS=128	
173	0.444829868	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.4? Tell 192.168.108.130	
174	0.444873287	192.168.108.1	192.168.108.130	TCP	74 80 - 41896 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM TSval=36947233 TSecr=324052...	
175	0.444911513	192.168.108.130	192.168.108.1	TCP	66 41896 - 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3240521697 TSecr=36947233	
176	0.444969805	192.168.108.130	192.168.108.1	TCP	66 41896 - 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3240521697 TSecr=36947233	

**Tương tự với địa chỉ .128**

Index	Source	Destination	Type	Length	Time	Content
230	0.676791889	192.168.108.130	192.168.108.128	TCP	74 45618 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=1351366590 TSecr=0 WS=128	
231	0.677203360	192.168.108.128	192.168.108.130	TCP	74 80 - 45618 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=436863 TSecr=1351366590 WS=32	
232	0.677244177	192.168.108.130	192.168.108.128	TCP	66 45618 - 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1351366591 TSecr=436863	
233	0.677309467	192.168.108.130	192.168.108.128	TCP	66 45618 - 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=1351366591 TSecr=436863	

Có một trường hợp đặc biệt là địa chỉ .254

Có thể gửi yêu cầu kết nối đến nhưng không có nhận được đáp lại

Index	Source	Destination	Type	Length	Time	Content
108	0.237901480	192.168.108.130	192.168.108.254	TCP	74 45624 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3119555991 TSecr=0 WS=128	
157	0.352789865	VMware_Bb:34:a8	Broadcast	ARP	42 Who has 192.168.108.127? Tell 192.168.108.130	
158	0.374776257	192.168.108.130	192.168.108.254	TCP	74 45632 - 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3119556128 TSecr=0 WS=128	

**OS Fingerprinting**

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ sudo nmap --min-rate=1000 -O 192.168.108.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 16:21 +07
Nmap scan report for 192.168.108.128
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:8B:D0:CD (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds
```

### Banner Grabbing/Service Enumeration

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ sudo nmap --min-rate=1000 -sV -T4 -A 192.168.108.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 16:26 +07
Nmap scan report for 192.168.108.128
Host is up (0.00088s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|   Connected to 192.168.108.130
|   logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:05:f6:a6:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-10-16T09:26:57+00:00; +8s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
```

#### ④ Bài tập về nhà (Yêu cầu làm)

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

Để xuất các cổng tcp và liệt kê các banner sử dụng câu lệnh sau:  
 sudo nmap –min-rate=1000 -sV -p- --script=banner <ip của Metasploitable 2>

Câu lệnh trên sử dụng nmap với option -sV(xuất version của dịch vụ đang chạy trên cổng đó).

-p- : Quét tất cả các cổng

--min-rate=1000 : nhằm để quét nhanh hơn

--script=banner : sử dụng script “banner” để xuất các banner

```
[(kali㉿kali)-[~/Documents/NT140/Lab02]]$ sudo nmap --min-rate=1000 -sV -p- --script=banner 192.168.108.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 16:29 +07
Nmap scan report for 192.168.108.128
Host is up (0.0013s latency).

Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_banner: 220 (vsFTPd 2.3.4)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp    open  telnet        Linux telnetd
|_banner: \xFF\xFD\x18\xFF\xFD\xFF\xFD#\xFF\xFD'
25/tcp    open  smtp         Postfix smtpd
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp    rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     33392/udp  mountd
|   100005  1,2,3     51453/tcp   mountd
|   100021  1,3,4     37472/tcp   nlockmgr
|   100021  1,3,4     57526/udp   nlockmgr
|   100024  1          34833/udp   status
|   100024  1          39759/tcp   status
```

## *Nmap Scripting Engine (NSE)*

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ nmap --min-rate=1000 192.168.108.128 --script=smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 16:35 +07
Nmap scan report for 192.168.108.128
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Host script results:
| smb-os-discovery:
|_ OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2024-10-16T05:35:59-04:00

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

**④ Bài tập về nhà (Yêu cầu làm)****33. Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)**

Sử dụng script “vuln” : Tập hợp các script kiểm tra lỗ hổng bảo mật phổ biến  
Kết quả trả về là các cve

## Lab 02: Information Gathering

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ nmap --min-rate=1000 -sV --script=vuln 192.168.108.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 18:32 +07
Nmap scan report for 192.168.108.128
Host is up (0.0025s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-vsftpd-backdoor:
| VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs: BID:48539 CVE:2011-2523
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:a:openbsd:openssh:4.7p1:
|     95499236-C9FE-56A6-9D7D-E943A24B633A  10.0  https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
|     2C119FFA-ECE0-5E14-A4A4-354A2C38071A  10.0  https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
|     CVE-2023-38408  9.8   https://vulners.com/cve/CVE-2023-38408
|     CVE-2016-1908  9.8   https://vulners.com/cve/CVE-2016-1908
|     B8190CDB-3EB9-5631-9828-8064A1575B23  9.8   https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
|     8FC9C5AB-3968-5F3C-825E-E8DB5379A623  9.8   https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
|     8AD01159-548E-546E-AA87-2DE89F3927EC  9.8   https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
|     5E6968B4-DBD6-57FA-BF6E-D9822190B27A  9.8   https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9822190B27A *EXPLOIT*
|     CVE-2015-5600  8.5   https://vulners.com/cve/CVE-2015-5600
|     SSV:78173  7.8   https://vulners.com/seebug/SSV:78173 *EXPLOIT*
|     SSV:69983  7.8   https://vulners.com/seebug/SSV:69983 *EXPLOIT*
|     PACKETSTORM:98796  7.8   https://vulners.com/packetstorm/PACKETSTORM:98796 *EXPLOIT*
|     PACKETSTORM:94556  7.8   https://vulners.com/packetstorm/PACKETSTORM:94556 *EXPLOIT*
|     PACKETSTORM:140070  7.8   https://vulners.com/packetstorm/PACKETSTORM:140070 *EXPLOIT*
|     PACKETSTORM:101052  7.8   https://vulners.com/packetstorm/PACKETSTORM:101052 *EXPLOIT*
|     EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985  7.8   https://vulners.com/exploitpack/EXPLOITPACK:71D51B69AA2D3A74753D7A921EE79985 *
|     EXPLOITPACK:67F6569F63A082199721C069C852BBD7  7.8   https://vulners.com/exploitpack/EXPLOITPACK:67F6569F63A082199721C069C852BBD7 *
|     EXPLOIT*
```

Sử dụng script “http-sql-injection”: Tự động kiểm tra lỗ hổng SQL Injection trên các dịch vụ web đang chạy.

Kết quả trả về sẽ là chi tiết những vị trí có khả năng bị lỗ hổng

```
(kali㉿kali)-[~/Documents/NT140/Lab02]
$ nmap --min-rate=1000 -sV --script=http-sql-injection 192.168.108.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-16 18:36 +07
Nmap scan report for 192.168.108.128
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-sql-injection:
| Possible sqli for queries:
|   http://192.168.108.128:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=documentation%2fhow-to-access-Mutillidae-over-Virtu
al-Box-network.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
|   http://192.168.108.128:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=documentation%2fvulnerabilities.php%27%20OR%20sqlsp
ider
|   http://192.168.108.128:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
|   http://192.168.108.128:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|   http://192.168.108.128:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
```