

Lab 1+2: THU THẬP THÔNG TIN

Thực hành môn Nhập môn bảo đảm và an ninh thông tin

Nhóm: 8

Lớp: IE105.O12.CNCL.1

Danh sách thành viên:

MSSV	Họ tên	Đánh giá
21522405	Nguyễn Thị Nhàn	Tốt
21522411	Trần Trọng Nhân	Tốt
21522557	Trần Thanh Sơn	Tốt
21522677	Nguyễn Trí Tín	Tốt
21522777	Trương Quang Tường	Tốt

1. Thu thập thông tin thụ động (Passive Information Gathering)

1. Từ trang web của MegaCorp One, hãy mô tả một chút về lĩnh vực hoạt động của công ty?
 - MegaCorp One chuyên về đổi mới đột phá trong ngành công nghệ nano và chịu trách nhiệm xác định các tiêu chuẩn trong ngành y tế, điện tử và thương mại.
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)?

MEET OUR TEAM



Joe Sheer
CHIEF EXECUTIVE OFFICER

Email: joe@megacorpone.com
Twitter: @Joe_Sheer



Tom Hudson
WEB DESIGNER

Email: thudson@megacorpone.com
Twitter: @TomHudsonMCO



Tanya Rivera
SENIOR DEVELOPER

Email: trivera@megacorpone.com
Twitter: @TanyaRiveraMCO



Matt Smith
MARKETING DIRECTOR

Email: msmith@megacorpone.com
Twitter: @MattSmithMCO

-
3. Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra điều gì?
 - Khi có được địa chỉ Email của các thành viên thuộc tổ chức thì nhóm nhận ra đều có chung đuôi mail là thuộc công ty megacorpone và đầu mail là tên của nhân viên.
 4. Sử dụng công cụ whois để xác định các name server của MegaCorp One.

```
(parallels@kali-linux-2022-2)-[~]
$ 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: 2023-06-13T18:08:24Z
Creation Date: 2013-01-22T23:01:00Z
Registry Expiry Date: 2024-01-22T23:01:00Z
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: 2022-12-12T10:59:28Z
```

- Các name server của MegaCorp One:
 - NS1.MEGACORPONE.COM
 - NS2.MEGACORPONE.COM
 - NS3.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?

```
(parallels@kali-linux-2022-2)-[~]
$ whois uit.edu.vn
This TLD has no whois server, but you can access the whois database at
http://www.vnnic.vn/en
```

- Sử dụng công cụ whois không thể tìm kiếm các thông tin của trường Đại học Công nghệ Thông tin (uit.edu.vn). Vì tên miền uit.edu.vn không đăng ký thông qua các tổ chức đăng ký tên miền (domain registrars). Thông tin về người hoặc tổ chức đăng ký tên miền được lưu trữ trong cơ sở dữ liệu công khai tại “<http://www.vnnic.vn/en>”. Dịch vụ whois cho phép người dùng truy vấn và xem thông tin này.

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

VNNIC INTERNET RESOURCE WHOIS INFORMATION

This whois query was received from IP Address: **42.116.127.217**
We recognize the resource in your query is: **Domain Name**
Type of domain name: **ASCII Domain Name**
Keyword in your query: **uit.edu.vn**

Domain information

Domain Name:	uit.edu.vn
Registrant Name:	Trường Đại học Công nghệ Thông tin
Registrar:	Công ty TNHH PA Việt Nam
Creation Date:	2006-10-02
Expiration Date:	2024-10-02
Status:	clientTransferProhibited
Nameserver:	ns1.pavietnam.vn ns2.pavietnam.vn nsbak.pavietnam.net
DNSSEC:	unsigned

- a. Ngày đăng ký tên miền: 02/10/2006
 - b. Ngày hết hạn tên miền: 02/10/2024
 - c. Chủ sở hữu tên miền: Trường Đại học Công nghệ Thông tin
 - d. Các name server của tên miền:
 - ns1.pavietnam.vn
 - ns2.pavietnam.vn
 - nsbak.pavietnam.net
7. Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?

Executive Team

Name: Joe Sheer

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@megacorpone.com

Contact Our Departments

Department: Human Resources

Email: hr@megacorpone.com

Department: Sales

Email: sales@megacorpone.com

Department: Shipping

Email: shipping@megacorpone.com

Our Address

MegaCorp One

2 Old Mill St
Rachel, NV 89001
United States.

Email: sales@megacorpone.com
Tel: (903) 883 - MEGA
Web: http://www.megacorpone.com

- Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One: Mike Carlow
- Địa chỉ email: mcarlow@megacorpone.com

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

The screenshot shows the RocketReach interface with a search bar containing the query "MegaCorp One". On the left, there are various filter options: Name, Location, Occupation, Role & Department, Skills, Years of Experience, Employer, Company Name or Domain, Intent, Employee Count, Revenue, Industry, Company Lists, Education, and Web. The results list includes:

- Mike Carlow, VP of Legal Affairs, MegaCorp One, Henderson, NV, US, with an email icon and a "Get Contact Info" button.
- Joe Sheer, Chief Executive Officer, Megacorp One, Alamo, Nevada, United States, with an email icon and a "Get Contact Info" button.
- Sam Hilker, Sales Associate, MegaCorp One, Wilmington, NC, US, with an email icon and a "Get Contact Info" button.
- Giovanni Kapo, Business Specialist, MegaCorp One, France, with an email icon and a "Get Contact Info" button.
- Steve Wong, System Administrator, MegaCorp One, Vancouver, BC, CA, with an email icon and a "Get Contact Info" button.
- Mutunga Muli, Electrical Specialist, MegaCorp One, Deadwood, SD, US, with an email icon and a "Get Contact Info" button.
- Emac Oscp, Senior Tester, MegaCorp One, Deadwood, SD, US, with an email icon and a "Get Contact Info" button.

Each result card also has a "View More" link. At the top right of the interface, there are buttons for "Upgrade Now", notifications, and other account settings.

- Một số nhân viên không được liệt kê trên trang web của MegaCorp One là:
 - Steve Wong – System Administrator
 - Sam Hilker – Sales Associate

- Vicuong Ha - Manager
- Giovanni Kapo – Business Specialist
- Mutunga Muli – Electrical Specialist
- Emac Oscp – Senior Tester

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

- Các từ khoá thường gặp trên Google là:

- Thời tiết
- Tin tức
- Xem phim
- Nhạc mới
- Sách hay
- Du lịch
- Mua sắm
- Công nghệ
- Học trực tuyến
- Công thức nấu ăn

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

- Một số tài liệu học tập của Trường theo nhóm chỉ nên được lưu hành nội bộ, không nên được công bố rộng rãi trên internet:


01 HÀN THUYỀN
 KP6, Linh Trung, Thủ Đức, TPHCM

CE@UIT.EDU.VN
 Hoạt động giờ hành chính

THỨ 2 - 6: 07G30 - 16G30
 Trực online 24/7

[TRANG CHỦ](#) [GIỚI THIỆU](#) [TUYỂN SINH](#) [CE DAY](#) [STUDENT HUB](#) [VIỆC LÀM](#) [SỰ KIỆN](#) [BIỂU MẪU](#) [LIÊN HỆ](#) [DMS](#)

KHO TÀI LIỆU SỐ

Vui lòng sử dụng **EMAIL UIT** để xem được tài liệu

All

Tìm môn học



Search for courses, books or documents

[Universities](#) [Books](#) [AI Questions](#) [Upgrade](#) [Save](#) [Share](#) [...](#)

Information **AI Chat**

Lab 1+2 – Information Gathering
 IE105

Course
 Nhập môn kĩ thuật (ME1001) 16 documents

University
 Hồ Chí Minh City University of Technology

[More info](#)

Recommended for you

- Ôn tập thi cuối kỳ I – Mạng máy tính – ĐHCNTT
- Nhập môn mạng máy tính – Practice materials 100% (5)
- BÀI TẬP VỀ THI Trong Toeic
- English Practical 100% (14)
- Successful Onboarding Strategies to Unlock Hidden Value Within Your...
- English Mandatory assignments 100% (3)

Download **AI Quiz** **0** **0** **Save** **Share**

Bộ môn An toàn Thông
 Trường Đại học Công nghệ TP
 Hồ Chí Minh

Was this document helpful? **0** **0**

1+2
Lab **PHỤC VỤ MỤC ĐÍCH GIÁO DỤC**

THU THẬP THÔNG TIN
 Information Gathering
 Thực hành môn Nhập môn bảo đảm và an ninh thông tin

Business partner hi workbank

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][whoxy_whois] > modules load recon/hosts-hosts/resolve
[recon-ng][default][resolve] > options set SOURCE www.megacorpone.com
SOURCE ⇒ www.megacorpone.com
[recon-ng][default][resolve] > run
[*] www.megacorpone.com ⇒ 149.56.244.87
[recon-ng][default][resolve] > options set SOURCE vpn.megacorpone.com
SOURCE ⇒ vpn.megacorpone.com
[recon-ng][default][resolve] > run
[*] vpn.megacorpone.com ⇒ 51.222.169.220
[recon-ng][default][resolve] > options set SOURCE siem.megacorpone.com
SOURCE ⇒ siem.megacorpone.com
[recon-ng][default][resolve] > run
[*] siem.megacorpone.com ⇒ 51.222.169.215
[recon-ng][default][resolve] > options set SOURCE www2.megacorpone.com
SOURCE ⇒ www2.megacorpone.com
[recon-ng][default][resolve] > run
[*] www2.megacorpone.com ⇒ 149.56.244.87
[recon-ng][default][resolve] > options set SOURCE intranet.megacorpone.com
SOURCE ⇒ intranet.megacorpone.com
[recon-ng][default][resolve] > run
[*] intranet.megacorpone.com ⇒ 51.222.169.211
[recon-ng][default][resolve] > options set SOURCE support.megacorpone.com
SOURCE ⇒ support.megacorpone.com
[recon-ng][default][resolve] > run
[*] support.megacorpone.com ⇒ 51.222.169.218
```

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

```

[*] [recon-ng][default] > marketplace install recon/domains-hosts/hackertarget
[*] [recon-ng][default] > modules load recon/domains-hosts/hackertarget
[*] [recon-ng][default][hackertarget] > options set SOURCE uit.edu.vn
SOURCE => uit.edu.vn
[*] [recon-ng][default][hackertarget] > run

UIT.EDU.VN
[*] Country: None
[*] Host: mx1.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: mapr2022.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: a084742fa316491c8c78564efcbce9e0-68f6236f-vm-80.vlab2.uit.edu.vn
[*] Ip_Address: 45.122.249.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: host2.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: mitaka.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: forumbeta.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: inseclab.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: api.mmllab.uit.edu.vn
[*] Ip_Address: 118.69.123.142
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: annotation.mmllab.uit.edu.vn
[*] Ip_Address: 118.69.123.142
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] _____
[*] Country: None
[*] Host: mx2.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: forum4.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: sois2017.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: mapr2018.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: daa.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] _____
[*] Country: None
[*] Host: vlab.uit.edu.vn
[*] Ip_Address: 45.122.249.74
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: 519bb137df6144dcbeda18e87d53ad8a-0-s-80.vlab.uit.edu.vn
[*] Ip_Address: 45.122.249.74
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: console-cloud.vlab.uit.edu.vn
[*] Ip_Address: 45.122.249.74
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: qttb.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: isccclub.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] _____
```

```
[*] _____
[*] Country: None
[*] Host: aiclub.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: qlhc.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: nc.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: dsc.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: cnsc.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: hcmcovidsafe.tech4covid.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: gw.tech4covid.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: hmcovidsafe-gw.tech4covid.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: fce.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: ecommerce.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: khtc.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: chungthuc.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: cd.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: tech4covid.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: hmcovidsafe.tech4covid.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: khoahoctre.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: se.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: esetupdate.uit.edu.vn
[*] Ip_Address: 118.69.123.142
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: live.uit.edu.vn
[*] Ip_Address: 42.116.11.16
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: extensivereading.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] _____  
[*] Country: None  
[*] Host: elearning.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: huongnghiepdhqg.uit.edu.vn  
[*] Ip_Address: 45.122.249.78  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: sdn.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: tuyensinh.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: auth.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]
```

```
[*] _____  
[*] Country: None  
[*] Host: openstack.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: link.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: notebook.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: dreamspark.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: portal.uit.edu.vn  
[*] Ip_Address: 45.122.249.78  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]
```

```
[*] _____  
[*] Country: None  
[*] Host: dbcl.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: phongdl.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: bandl.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: congdoanql.uit.edu.vn  
[*] Ip_Address: 45.122.249.78  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: acm.uit.edu.vn  
[*] Ip_Address: 45.122.249.78  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None
```

```
[*] _____  
[*] Country: None  
[*] Host: tracnghiem.uit.edu.vn  
[*] Ip_Address: 45.122.249.78  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: forum.uit.edu.vn  
[*] Ip_Address: 45.122.249.78  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: debian.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: congdoan.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] _____  
[*] Country: None  
[*] Host: khcn.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]
```

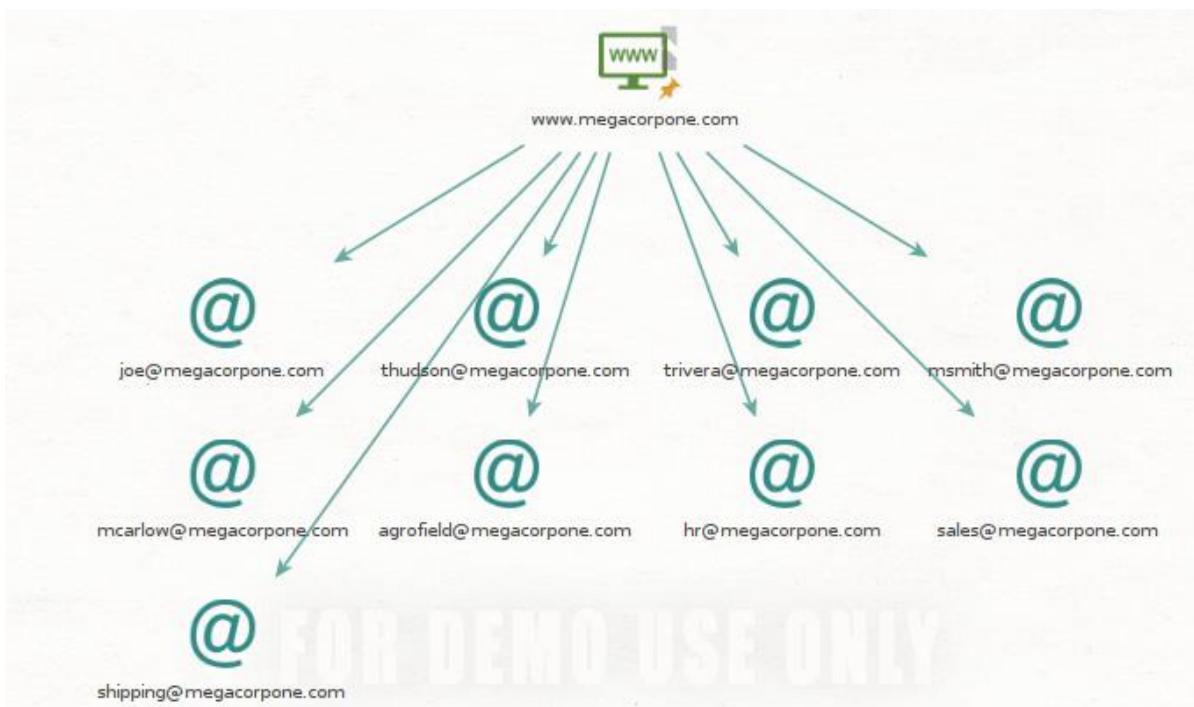
```
[*] _____
[*] Country: None
[*] Host: qhdn.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: en.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: thuvien.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: www.thuvien.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: cybertrain.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: doantn.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: dangbo.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: huongghiep.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: oep.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: demodkhp.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
```

```
[*] _____
[*] Country: None
[*] Host: nlp.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: ftp.uit.edu.vn
[*] Ip_Address: 42.116.6.44
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: hostmaster.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: mapr.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: sonaas.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: cs.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: aiclub.cs.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: service.aiclub.cs.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: student.cs.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
[*] Country: None
[*] Host: banqlcs.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] _____
```

```
[*] Country: None
[*] Host: courses.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: oms.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: netsens.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: photos.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: qldt.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Region: None
[**] Country: None
[*] Host: mmt.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: ktmt.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: student.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: iot.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: app1.iot.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: eset.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: ctgt.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: fit.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: git.uit.edu.vn
[*] Ip_Address: 118.69.123.138
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: khmt.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Region: None
[**] Country: None
[*] Host: testbed.iot.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: forum.iot.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: httt.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: ecommerce.httt.uit.edu.vn
[*] Ip_Address: 118.69.123.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[**] Country: None
[*] Host: ptnhtt.uit.edu.vn
[*] Ip_Address: 45.122.249.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

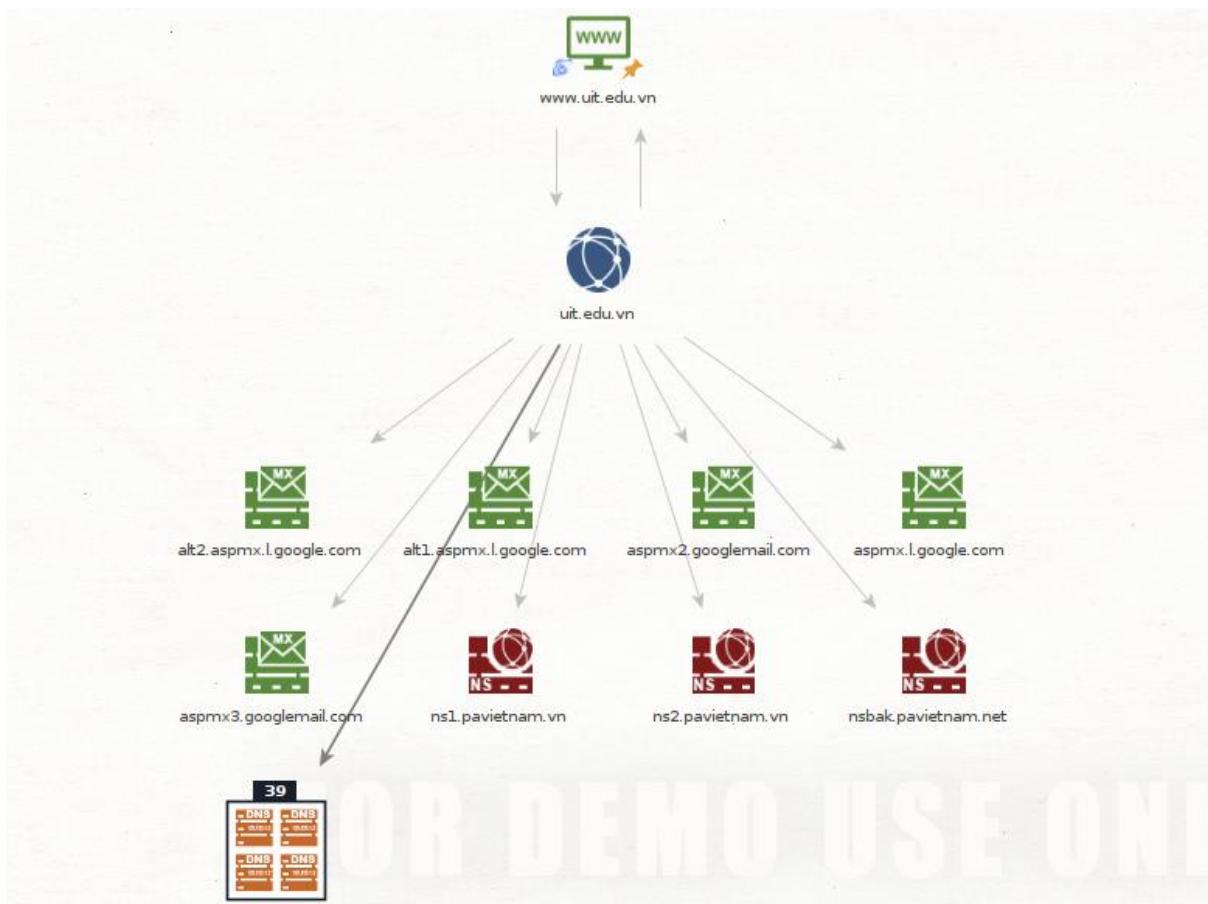
```
[*] Country: None  
[*] Host: ctsv.uit.edu.vn  
[*] Ip_Address: 45.122.249.78  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: www.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: ceday.uit.edu.vn  
[*] Ip_Address: 118.69.123.140  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: danguy.uit.edu.vn  
[*] Ip_Address: 45.122.249.78  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]
```

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

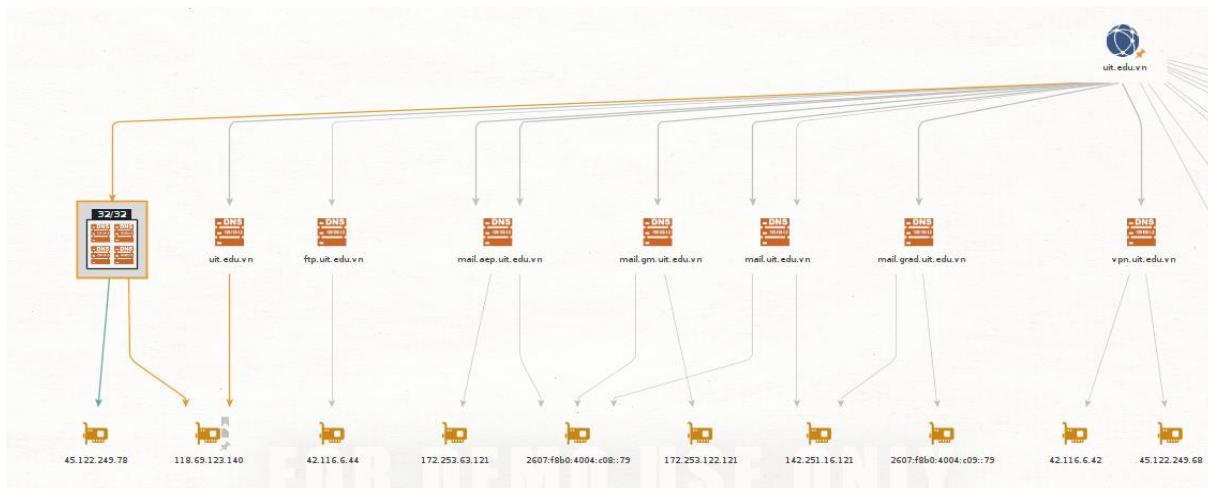


20. Sử dụng công cụ Maltego cho UIT (tên miền: uit.edu.vn) và trả lời các câu hỏi sau:

a. Các bản ghi DNS.



b. Các website và địa chỉ IP tương ứng.



- 32 website có địa chỉ IP là 45.122.249.78 và 118.69.123.140

1	app2.uit.edu.vn
2	cybertrain-2.uit.edu.vn
3	de.uit.edu.vn
4	dmz.uit.edu.vn
5	dns.uit.edu.vn
6	doantn.uit.edu.vn
7	extranet.uit.edu.vn
8	fit.uit.edu.vn
9	forum.uit.edu.vn
10	fr.uit.edu.vn
11	frodo.uit.edu.vn
12	gateway.uit.edu.vn
13	green.uit.edu.vn
14	host2.uit.edu.vn
15	is.uit.edu.vn
16	iscclub.uit.edu.vn
17	mx.uit.edu.vn
18	ns1.uit.edu.vn
19	orange.uit.edu.vn
20	pop.uit.edu.vn
21	smith.uit.edu.vn
22	smtp.uit.edu.vn
23	tcvaccine.uit.edu.vn
24	trinity.uit.edu.vn
25	uk.uit.edu.vn
26	venus.uit.edu.vn
27	vpn1.uit.edu.vn
28	wildcard-in-use.uit.edu.vn
29	www.de.uit.edu.vn
30	www.service.aiclub.cs.uit.edu.vn
31	www.uit.edu.vn
32	www.uk.uit.edu.vn

2. Thu thập thông tin chủ động (Active Information Gathering)

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

- **AAAA**: Tương đồng với bản ghi A nhưng trả đến một địa chỉ IPv6 của máy chủ DNS.
- **SOA (Start of Authority)**: Bản ghi SOA lưu trữ thông tin quan trọng về các miền và được sử dụng để giám sát lưu lượng giữa các nameserver chính và thứ cấp.
- **SRV (Service)**: Bản ghi SRV được sử dụng để xác định vị trí các dịch vụ đặc biệt trong một tên miền.
- **SPF (Sender Policy Framework)**: Bản ghi SPF đảm bảo các máy chủ mail sẽ chấp nhận mail từ tên miền của máy khách chỉ được gửi đi từ server của máy khách, giúp chống spam và giả mạo email.
- **HINFO (Host Information)**: Bản ghi HINFO cung cấp thông tin về phần cứng và hệ điều hành của máy chủ được liên kết với tên miền.
- **LOC (Location)**: Bản ghi LOC cung cấp thông tin về vị trí địa lý của máy chủ được liên kết với tên miền.
- **NAPTR (Naming Authority Pointer)**: Bản ghi NAPTR cho phép định cấu hình cách giải quyết tên miền cho các dịch vụ không được hỗ trợ bởi các bản ghi DNS tiêu chuẩn.
- **KX (Key Exchange)**: Bản ghi KX được sử dụng để định cấu hình máy chủ DNS chính thức cho miền.
- **CAA (Certification Authority Authorization)**: Bản ghi CAA cho phép chỉ định các cơ quan chứng nhận (CA) được phép cấp chứng chỉ SSL cho tên miền.
- **TLSA (TLS Authentication)**: Bản ghi TLSA cung cấp thông tin về các khóa được sử dụng để mã hóa kết nối TLS cho tên miền.

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

```
root@kali: ~
File Actions Edit View Help

[~]# host -t txt uit.edu.vn
uit.edu.vn descriptive text "k6t321pqvf9jryb0z4n5scftqph6t781"
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"
uit.edu.vn descriptive text "google-site-verification=z9wIF5gp5-YbdAQsttR2Kmy
HCPy3FN6QkOGOBUIrwc"
uit.edu.vn descriptive text "svp60rjlwr6s19rn9t013cfwm3xmqx7h"
uit.edu.vn descriptive text "sqm6y27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C91t
Pny8NLttGS0aU5pJjKiY"

[~]# host -t mx uit.edu.vn
uit.edu.vn mail is handled by 40 aspmx3.googlemail.com.
uit.edu.vn mail is handled by 20 alt2.aspmx.l.google.com.
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.

[~]#
```

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?

```
root@kali: ~
File Actions Edit View Help

[~]# host noexist.uit.edu.vn
noexist.uit.edu.vn has address 118.69.123.140
noexist.uit.edu.vn has address 45.122.249.78

[~]# host idontexist.uit.edu.vn
idontexist.uit.edu.vn has address 45.122.249.78
idontexist.uit.edu.vn has address 118.69.123.140

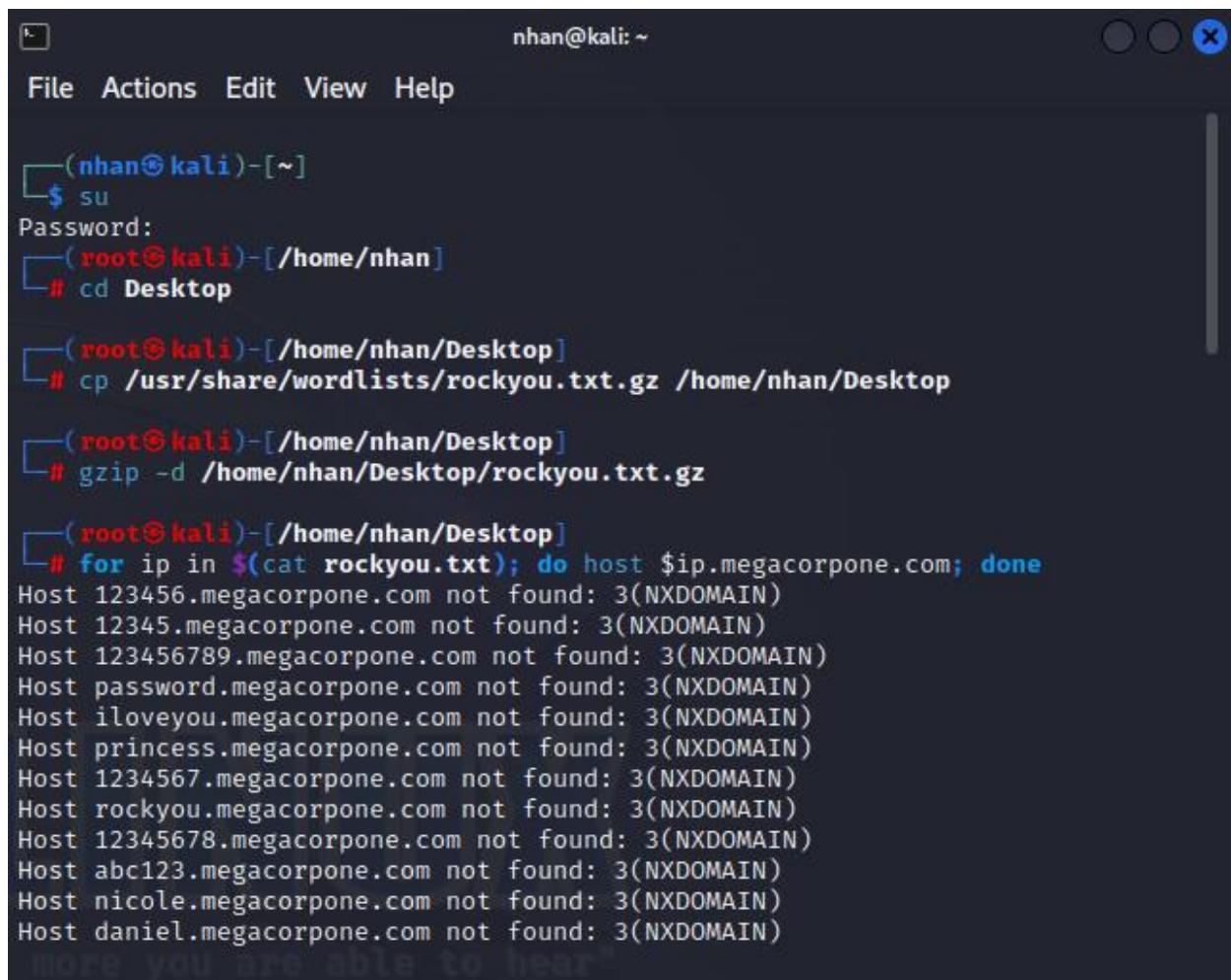
[~]# host baithuchanhso2.uit.edu.vn
baithuchanhso2.uit.edu.vn has address 118.69.123.140
baithuchanhso2.uit.edu.vn has address 45.122.249.78

[~]#
```

- Thực hiện truy vấn các hostname không tồn tại và nhận được các địa chỉ IP tương ứng là 118.69.123.140 và 45.122.249.78 có thể là kết quả của một số cấu hình DNS đặc biệt. Hệ thống DNS có thể sử dụng wildcard để ánh xạ mọi hostname chưa được xác định đến một địa chỉ IP cụ thể. Điều này có thể dẫn đến việc nhận được địa chỉ IP thay vì thông báo lỗi.

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

- Sử dụng wordlist *rockyou*:



```

nhan@kali: ~
File Actions Edit View Help

└─(nhan㉿kali)-[~]
$ su
Password:
└─(root㉿kali)-[/home/nhan]
# cd Desktop

└─(root㉿kali)-[/home/nhan/Desktop]
# cp /usr/share/wordlists/rockyou.txt.gz /home/nhan/Desktop
# gzip -d /home/nhan/Desktop/rockyou.txt.gz

└─(root㉿kali)-[/home/nhan/Desktop]
# for ip in $(cat rockyou.txt); do host $ip.megacorpone.com; done
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)
more you are able to hear

```

- Sử dụng wordlist namelist.txt trong seclists:

```
root@kali: /usr/share/seclists
File Actions Edit View Help
└─(root㉿kali)-[/usr/share/seclists]
  └─# ls /usr/share/seclists/Discovery/DNS
    README.md
    bitquark-subdomains-top100000.txt
    bug-bounty-program-subdomains-trickest-inventory.txt
    combined_subdomains.txt
    deepmagic.com-prefixes-top500.txt
    deepmagic.com-prefixes-top50000.txt
    dns-Jhaddix.txt
    fierce-hostlist.txt
    italian-subdomains.txt
    n0kovo_subdomains.txt
    namelist.txt
    shubs-stackoverflow.txt
    shubs-subdomains.txt
    sortedcombined-knock-dnsrecon-fierce-reconng.txt
    subdomains-spanish.txt
    subdomains-top1million-110000.txt
    subdomains-top1million-20000.txt
    subdomains-top1million-5000.txt
    tlds.txt

└─(root㉿kali)-[/usr/share/seclists]
  └─# cp /usr/share/seclists/Discovery/DNS/namelist.txt /home/nhan/Desktop
└─(root㉿kali)-[/usr/share/seclists]
  └─#
```

```
root@kali: /home/nhan/Desktop
File Actions Edit View Help
└─(root㉿kali)-[/home/nhan/Desktop]
  └─# for ip in $(cat namelist.txt); do host $ip.megacorpone.com; done
Host 0.megacorpone.com not found: 3(NXDOMAIN)
Host 01.megacorpone.com not found: 3(NXDOMAIN)
Host 02.megacorpone.com not found: 3(NXDOMAIN)
Host 03.megacorpone.com not found: 3(NXDOMAIN)
Host 1.megacorpone.com not found: 3(NXDOMAIN)
Host 10.megacorpone.com not found: 3(NXDOMAIN)
Host 11.megacorpone.com not found: 3(NXDOMAIN)
Host 12.megacorpone.com not found: 3(NXDOMAIN)
Host 13.megacorpone.com not found: 3(NXDOMAIN)
Host 14.megacorpone.com not found: 3(NXDOMAIN)
Host 15.megacorpone.com not found: 3(NXDOMAIN)
Host 16.megacorpone.com not found: 3(NXDOMAIN)
Host 17.megacorpone.com not found: 3(NXDOMAIN)
Host 18.megacorpone.com not found: 3(NXDOMAIN)
Host 19.megacorpone.com not found: 3(NXDOMAIN)
Host 2.megacorpone.com not found: 3(NXDOMAIN)
Host 20.megacorpone.com not found: 3(NXDOMAIN)
Host 3.megacorpone.com not found: 3(NXDOMAIN)
Host 3com.megacorpone.com not found: 3(NXDOMAIN)
Host 4.megacorpone.com not found: 3(NXDOMAIN)
Host 5.megacorpone.com not found: 3(NXDOMAIN)
Host 6.megacorpone.com not found: 3(NXDOMAIN)
Host 7.megacorpone.com not found: 3(NXDOMAIN)
Host 8.megacorpone.com not found: 3(NXDOMAIN)
```

23. Viết một chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM (`hcmus.edu.vn`, `hcmussh.edu.vn`, `uit.edu.vn`, `hcmut.edu.vn`, `hcmiu.edu.vn`, `uel.edu.vn`, `hcmier.edu.vn`, `vnuhcm.edu.vn`) và thực hiện zone transfer ứng với các nameserver đã tìm được.

- Chương trình Bash script để liệt kê danh sách các nameserver của các đơn vị thành viên thuộc Đại học Quốc Gia TP.HCM:

```
root@kali: /home/nhan/Desktop
File Actions Edit View Help

[(root㉿kali)-[~/Desktop]]# 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"); for domain in "${domains[@]}"; do nameservers=$(host -t ns "$domain"); echo "$nameservers"; done

hcmus.edu.vn name server dns2.hcmus.edu.vn.
hcmus.edu.vn name server dns1.hcmus.edu.vn.
hcmus.edu.vn name server server.hcmus.edu.vn.
hcmussh.edu.vn name server ns2.vdconline.vn.
hcmussh.edu.vn name server ns1.vdconline.vn.
uit.edu.vn name server ns1.pavietnam.vn.
uit.edu.vn name server ns2.pavietnam.vn.
uit.edu.vn name server nsbak.pavietnam.net.
hcmut.edu.vn name server dns2.hcmut.edu.vn.
hcmut.edu.vn name server dns4.hcmut.edu.vn.
hcmut.edu.vn name server dns3.hcmut.edu.vn.
hcmut.edu.vn name server dns1.hcmut.edu.vn.
hcmiu.edu.vn name server vdc-hn01.vnn.vn.
hcmiu.edu.vn name server hcm-server1.vnn.vn.
uel.edu.vn name server ns2.dns.net.vn.
uel.edu.vn name server ns1.dns.net.vn.
hcmier.edu.vn name server server.vnuhcm.edu.vn.
hcmier.edu.vn name server vnuserv.vnuhcm.edu.vn.
vnuhcm.edu.vn name server server.vnuhcm.edu.vn.
vnuhcm.edu.vn name server ns1.vdc2.vn.
vnuhcm.edu.vn name server vnuserv.vnuhcm.edu.vn.
vnuhcm.edu.vn name server ns2.vdc2.vn.

[(root㉿kali)-[~/Desktop]]#
```

- Thực hiện zone transfer với các nameserver của vnuhcm.edu.vn:

```
root@kali: /home/nhan/Desktop
File Actions Edit View Help

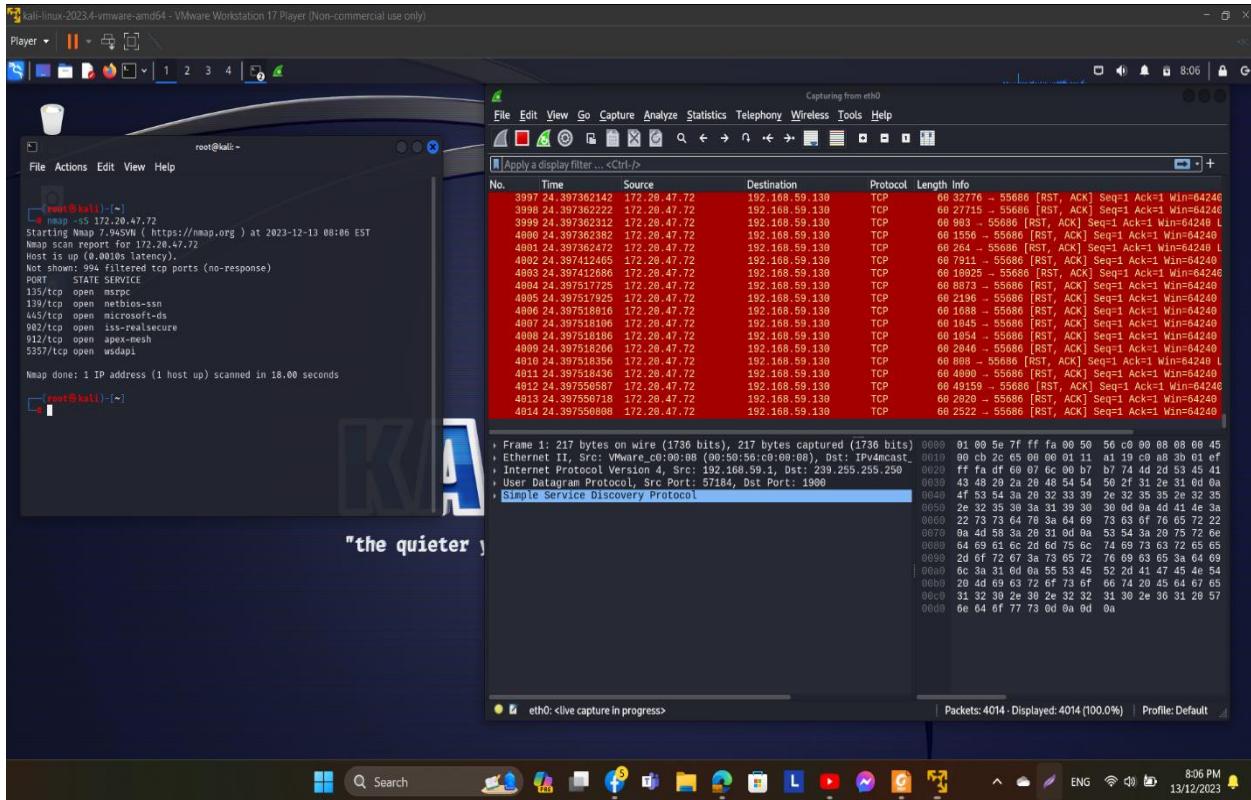
[ (root㉿kali)-[~/Desktop] ]
# host -l vnuhcm.edu.vn ns1.vdc2.vn
Using domain server:
Name: ns1.vdc2.vn
Address: 14.225.232.25#53
Aliases:

Host vnuhcm.edu.vn not found: 5(REFUSED)
; Transfer failed.

[ (root㉿kali)-[~/Desktop] ]
# host -l vnuhcm.edu.vn ns2.vdc2.vn
Using domain server:
Name: ns2.vdc2.vn
Address: 14.225.232.26#53
Aliases:

vnuhcm.edu.vn name server vnuserv.vnuhcm.edu.vn.
vnuhcm.edu.vn name server server.vnuhcm.edu.vn.
vnuhcm.edu.vn has address 103.88.121.29
www.4s.vnuhcm.edu.vn has address 118.69.204.199
aaa.vnuhcm.edu.vn has address 103.88.123.21
aaa1.vnuhcm.edu.vn has address 103.88.123.22
aad.vnuhcm.edu.vn has address 203.162.44.60
ab.vnuhcm.edu.vn has address 203.162.147.252
aun.vnuhcm.edu.vn has address 203.162.147.168
baixeektx.vnuhcm.edu.vn has address 123.30.236.140
baocaoaad.vnuhcm.edu.vn has address 203.162.44.60
mssql.baocaoaad.vnuhcm.edu.vn has address 203.162.44.60
betaaad.vnuhcm.edu.vn has address 222.255.69.252
cdio2015.vnuhcm.edu.vn has address 221.133.13.127
cea.vnuhcm.edu.vn has address 103.88.123.7
csgd.cea.vnuhcm.edu.vn has address 103.88.123.7
database.cea.vnuhcm.edu.vn has address 103.88.123.7
dkht.cea.vnuhcm.edu.vn has address 103.88.123.7
cete.vnuhcm.edu.vn has address 103.88.123.2
chrd.vnuhcm.edu.vn has address 203.162.147.149
club.vnuhcm.edu.vn has address 203.162.147.185
www.cnttt.vnuhcm.edu.vn has address 203.162.44.72
congdoan.vnuhcm.edu.vn has address 118.69.123.142
cpmu-demo.vnuhcm.edu.vn has address 103.88.121.59
cpmu-demo1.vnuhcm.edu.vn has address 112.78.11.146
```

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



- Khi thực hiện SYN Scan (-sS) bằng Nmap, gói tin được gửi và nhận theo các bước sau:

1) Gửi gói tin SYN (Synchronize):

- Nmap bắt đầu bằng việc gửi gói tin SYN đến cổng đích trên máy mục tiêu.
- Gói tin SYN có nhiệm vụ bắt đầu quá trình thiết lập kết nối TCP bằng cách yêu cầu mở một kết nối, nhưng không hoàn tất quá trình.

2) Nhận gói tin SYN/ACK (Synchronize/Acknowledge) hoặc RST (Reset):

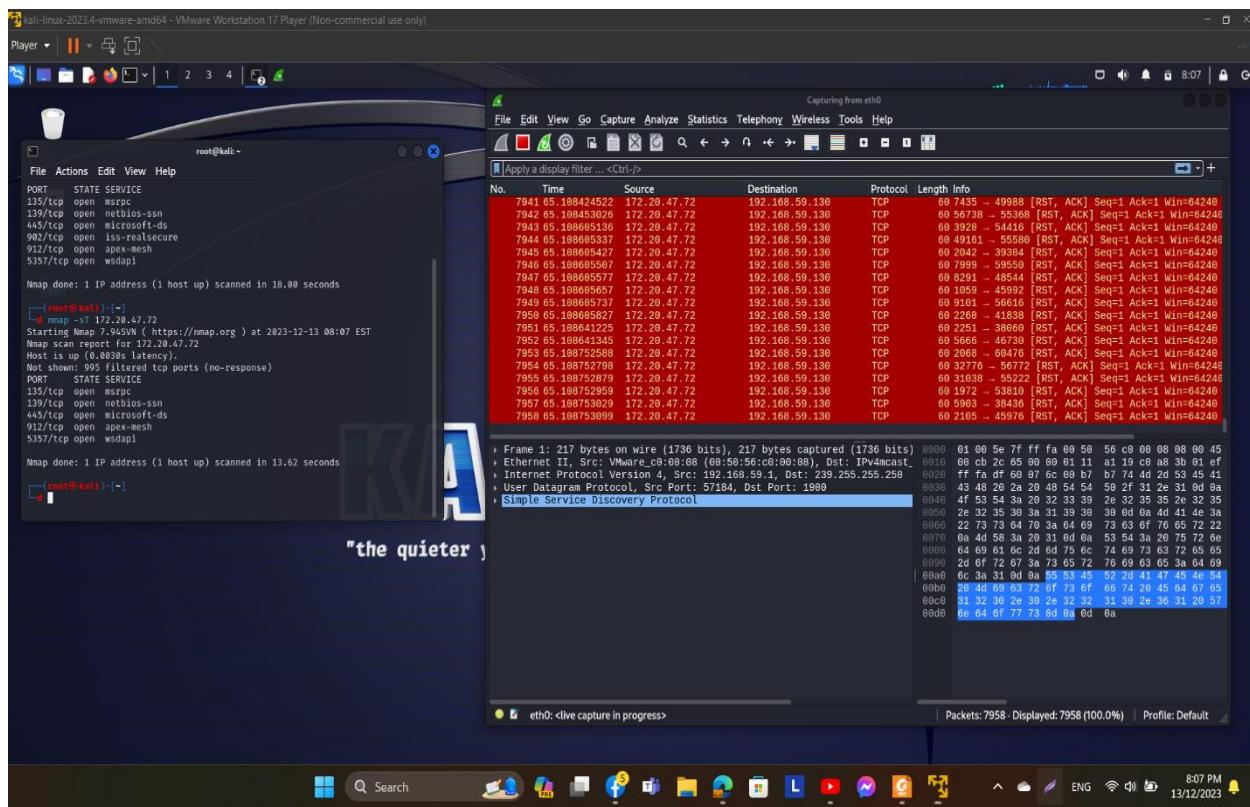
- Nếu cổng đích đang mở, máy chủ sẽ trả lời bằng gói tin SYN/ACK để xác nhận yêu cầu mở kết nối và yêu cầu xác nhận ACK.
- Nếu cổng đích đang đóng, máy chủ có thể trả lời bằng gói tin RST để đặt lại trạng thái kết nối và báo hiệu rằng cổng đang đóng.

3) Gửi gói tin RST (Reset) (nếu cổng đích mở): Nmap không gửi gói tin ACK, thay vào đó gửi gói tin RST làm cho kết nối bị ngắt trước khi hoàn tất quá trình bắt tay ba bước.

4) Hiển thị kết quả:

- Dựa vào phản hồi từ máy chủ, Nmap sẽ xác định xem cổng đích là mở hay đóng.
- Nmap cũng có thể xác định loại dịch vụ đang chạy trên cổng đó bằng cách kiểm tra danh sách các cổng phổ biến và dịch vụ tương ứng.

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



- Khi thực hiện TCP Connect Scan (-sT) bằng Nmap, gói tin được gửi và nhận theo các bước sau:

1) Gửi gói tin SYN (Synchronize):

- Nmap bắt đầu bằng việc gửi gói tin SYN đến cổng đích trên máy mục tiêu.
- Gói tin SYN có nhiệm vụ bắt đầu quá trình thiết lập kết nối TCP bằng cách yêu cầu mở một kết nối.

2) Nhận gói tin SYN/ACK (Synchronize/Acknowledge) hoặc RST (Reset):

- Nếu cổng đích đang mở, máy chủ sẽ trả lời bằng gói tin SYN/ACK để xác nhận yêu cầu mở kết nối. Gói tin này cũng chứa một số xác nhận ACK.
- Nếu cổng đích đang đóng, máy chủ có thể trả lời bằng gói tin RST để đặt lại trạng thái kết nối và báo hiệu rằng cổng đang đóng.

3) Gửi gói tin ACK (Acknowledge) (nếu cổng đích mở): Nmap gửi gói tin ACK để hoàn tất việc kết nối.

4) Gửi gói tin RST (Reset) (nếu cổng đích mở): Khi quá trình bắt tay hoàn tất, Nmap gửi gói RST để kết thúc kết nối.

5) Hiển thị kết quả:

- Dựa vào phản hồi từ máy chủ, Nmap sẽ xác định xem cổng đích là mở hay đóng.
- Nmap cũng có thể xác định loại dịch vụ đang chạy trên cổng đó bằng cách kiểm tra danh sách các cổng phổ biến và dịch vụ tương ứng.

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...)

- Dựa vào ảnh của câu 27 và câu 28 ta có bảng so sánh sau:

	SYN Scan	TCP Connect Scan
Số lượng gói tin được gửi	Ít gói tin hơn vì Nmap chỉ gửi các gói tin SYN để kiểm tra trạng thái cổng mà không hoàn tất quá trình kết nối TCP.	Nhiều gói tin hơn vì Nmap sẽ hoàn tất kết nối TCP bằng cách gửi gói tin ACK và kết thúc kết nối bằng cách gửi gói tin RST.

Số lượng gói tin được nhận	Chỉ nhận phản hồi từ các gói tin SYN/ACK hoặc RST.	Sẽ có thêm gói tin trong quá trình thiết lập kết nối TCP.
Thời gian quét	18.00 giây	13.62 giây
Kết quả hiển thị	Hiển thị trạng thái cổng (mở/đóng), dịch vụ và các thông tin khác.	

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

```
report bugs to <upstart-devel@lists.ubuntu.com>
nsfadmin@metasploitable:~$ shutdown -h
shutdown: time expected
try shutdown --help' for more information.
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:e2:f0:96
          inet addr:192.168.83.129  Bcast:192.168.83.255  Mask:255.255.
          inet6 addr: fe00::20c:29ff:fe2:f096/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:43 errors:0 dropped:0 overruns:0 frame:0
            TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5060 (4.9 KB)  TX bytes:13669 (13.3 KB)
            Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:351 errors:0 dropped:0 overruns:0 frame:0
            TX packets:351 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:148809 (145.3 KB)  TX bytes:148809 (145.3 KB)

nsfadmin@metasploitable:~$
```

```
[root@kali:~]
# nmap -ST -sV -A 192.168.83.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-15 00:37 +07
Nmap scan report for 192.168.83.129
Host is up (0.00005s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  vsftpd  2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.83.128
|   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
22/tcp    open  ssh       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cfe1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:b2:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet   Linux telnetd
```

```
[Metasploitable2-Linux - VMware Workstation 17 Player] Player [File Actions Edit View Help]
[report bugs to <upstart-devel@lists.ubuntu.com>
root@kali: ~]
[ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:e2:f0:96
          inet addr:192.168.0.3.129  Bcast:192.168.0.255  Mask:255.255.
          inet6 addr: fe80::20c:29ff:fe2:f096/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:43 errors:0 dropped:0 overruns:0 frame:0
            TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:5060 (4.9 KB)  TX bytes:13669 (13.3 KB)
            Interrupt:17  Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:351 errors:0 dropped:0 overruns:0 frame:0
            TX packets:351 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:148809 (145.3 KB)  TX bytes:148809 (145.3 KB)

root@kali: ~]
[File Actions Edit View Help]
[File Actions Edit View Help]
[25/tcp  open  smtp   Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
|_ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu0804-base.localdomain/organizationName=0
COSA/StateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp  open  domain  ISC BIND 9.4.2
|dns-nsid:
|_bind.version: 9.4.2
80/tcp  open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|http-title: Metasploitable2 - Linux
|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 33838/udp mounted
|_100005 1,2,3 44228/tcp mounted
|_100021 1,3,4 35159/tcp nlockmgr
|_100021 1,3,4 58841/udp nlockmgr
|_100024 1 56031/udp status
|_100024 1 57440/tcp status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
<the quieter you become, the more you are able to hear>
[File Actions Edit View Help]
```

```

Report bugs to <upstart-devel@lists.ubuntu.com>
nsadmin@metasploitable:~$ shutdown -h
shutdown: time expected
Try 'shutdown --help' for more information.
nsadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:e2:f0:96
          inet addr:192.168.83.129  Bcast:192.168.83.255  Mask:255.255.
          inet6 addr: fe80::20c:29ff:fee2:f096/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:43 errors:0 dropped:0 overruns:0 frame:0
             TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:5060 (4.9 KB)  TX bytes:13669 (13.3 KB)
             Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING  MTU:16436  Metric:1
             RX packets:351 errors:0 dropped:0 overruns:0 frame:0
             TX packets:351 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:148809 (145.3 KB)  TX bytes:148809 (145.3 KB)

nsadmin@metasploitable:~$ 

```

"the quieter you become, the more you are able to hear"

```

File Actions Edit View Help
445/tcp open      Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open      exec      netkit-rsh rexecd
513/tcp open      login?
514/tcp open      shell      Netkit rshd
1099/tcp open     java-rmi  GNU Classpath grmiregistry
1524/tcp open     bindshell  Metasploitable root shell
2049/tcp open     nfs       2-4 (RPC #100003)
2121/tcp open     ftp       ProFTPD 1.3.1
3306/tcp open     mysql     MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities Flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, SupportsTransactions, S
peaks41ProtocolNew, SupportsCompression, SwitchToSSLAfterHandshake, ConnectWi
thDatabase
|   Status: Autocommit
|   Salt: (M?Qq1=3+s)oswxpxPHV
5432/tcp open    postgresl PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=0
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| ssl-date: 2023-12-14T17:38:41+00:00; +5s from scanner time.
5900/tcp open    vnc      VNC (protocol 3.3)
| vnc-info:

```

```

Report bugs to <upstart-devel@lists.ubuntu.com>
nsadmin@metasploitable:~$ shutdown -h
shutdown: time expected
Try 'shutdown --help' for more information.
nsadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:e2:f0:96
          inet addr:192.168.83.129  Bcast:192.168.83.255  Mask:255.255.
          inet6 addr: fe80::20c:29ff:fee2:f096/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:43 errors:0 dropped:0 overruns:0 frame:0
             TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:5060 (4.9 KB)  TX bytes:13669 (13.3 KB)
             Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING  MTU:16436  Metric:1
             RX packets:351 errors:0 dropped:0 overruns:0 frame:0
             TX packets:351 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:148809 (145.3 KB)  TX bytes:148809 (145.3 KB)

nsadmin@metasploitable:~$ 

```

"the quieter you become, the more you are able to hear"

```

File Actions Edit View Help
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:E2:F0:96 (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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)

```

- Danh sách các dịch vụ TCP đang chạy trên máy Metasploitable 2:

Port	Dịch vụ
21	ftp
22	ssh
23	telnet
25	smtp
53	domain
80	http
111	rpcbind
139	netbios-ssn

445	
512	exec
513	login?
514	shell
1099	java-rmi
1524	bindshell
2049	nfs
2121	ftp
3306	mysql
5432	postgresql
5900	vnc
6000	X11
6667	irc
8009	ajp13
8180	http

33. Sử dụng thêm 2 NSE script (tự chọn) để quét máy mục tiêu (Metasploitable 2)

- Sử dụng NSE Script: http-title, dns-zone-transfer

Metasploitable2-Linux - VMware Workstation 17 Player

Player | < > | File Actions Edit View Help

```
report bugs to <upstart-devel@lists.ubuntu.com>
root@kali:~#
sfadmin@metasploitable:~$ shutdown -h
shutdown: time expected
try 'shutdown --help' for more information.
root@kali:~#
sfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:e2:f0:96
          inet6 addr: fe00::20c:29ff:fe09:64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5060 (4.9 KB)  TX bytes:13669 (13.3 KB)
          Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:351 errors:0 dropped:0 overruns:0 frame:0
          TX packets:351 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:148809 (145.3 KB)  TX bytes:148809 (145.3 KB)

sfadmin@metasploitable:~$ _
```

File Actions Edit View Help

```
[root@kali:~]
# nmap -sT -sV --script http-title,dns-zone-transfer 192.168.83.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-15 01:09 +07
Nmap scan report for 192.168.83.129
Host is up (0.00077s 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 smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|   program version  port/proto  service
|   10000  2          111/tcp    rpcbind
|   10000  2          111/udp   rpcbind
|   10003  2,3,4     2049/tcp   nfs
|   10003  2,3,4     2049/udp   nfs
|   10005  1,2,3     3838/udp   mountd
|   10005  1,2,3     4422/tcp   mountd
|   10021  1,3,4     35159/tcp   nlockmgr
|   10021  1,3,4     58841/udp   nlockmgr
```

- Sử dụng NSE Script: vuln, exploit

```
root@kali:~# nmap -sT -sV --script vuln,exploit 192.168.83.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-15 01:17 +07
Nmap scan report for 192.168.83.129
Host is up (0.0012s 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: CVE:2011-2523 BID:48539
|       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
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://www.securityfocus.com/bid/48539
|     vulners:
|       cpe:/a:vsftpd:vsftpd:2.3.4:           PRION:CVE-2011-2523      10.0      https://vulners.com/prion/PRION:CVE-2011-2523
|         EDB-ID:49757      10.0      https://vulners.com/exploitdb/EDB-ID:49757  *
EXPLOIT*
|       1337DAY-ID-36095      10.0      https://vulners.com/zdt/1337DAY-ID-36095  *EXPLOIT*
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     SSV:78173      7.8      https://vulners.com/seebug/SSV:78173      *EXPLOIT*
|     SSV:69983      7.8      https://vulners.com/seebug/SSV:69983      *EXPLOIT*
|     EDB-ID:24450      7.8      https://vulners.com/exploitdb/EDB-ID:24450  *EXPLOIT*
```