

BÁO CÁO THỰC HÀNH

Môn học: AN TOÀN MẠNG

Tên chủ đề: THU THẬP THÔNG TIN – INFORMATION GATHERING

GVHD: Tô Trọng Nghĩa

Nhóm: 21

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: XXX

STT	Họ và tên	MSSV	Email
01	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn
02	Nguyễn Thị Thanh Mai	21521112	21521112@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
01	Thu thập thông tin thụ động (câu 01 – câu 20)	95%	02 – 19
02	Thu thập thông tin chủ động (câu 21 – câu 35)	100%	19 – 38
Điểm tự đánh giá			9.5-10/10

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

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. THU THẬP THÔNG TIN THỤ ĐỘNG

a, Do thám Website (Website Reconnaissance)

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

→ Trả lời: Công ty MegaCorp One là một công ty chuyên về đổi mới đột phá trong ngành công nghệ nano. Họ chịu trách nhiệm xác định các tiêu chuẩn của ngành trong lĩnh vực y tế, điện tử và thương mại.

The screenshot shows the homepage of the website 'MegaCorp One'. At the top, there is a dark header bar with the company name 'MegaCorp One' in white. Below it, a navigation menu includes 'HOME', 'ABOUT' (which is highlighted in blue), 'CONTACT', 'SUPPORT', 'CAREERS', and 'LOG IN'. The main content area has a light blue background and features a large heading 'About Us' in bold. Below this, there is a paragraph of text followed by several short bullet points. At the bottom of the page, there is a footer section with some social media links.

MegaCorp One

HOME ABOUT CONTACT SUPPORT CAREERS LOG IN

About Us

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

Our success begins with the assessment of small teams working on independent project. Once we have selected a project that we believe will succeed, we procure their talent and refine the technology toward our common goals.

The ability to discover and encourage the brightest minds in the industry, has led to our rapidly increasing growth.

Chief Executive Officer, Joe Sheer, has been featured in the Journal of NanoTimes stating:

Our team is creating the building blocks of modern society, where technology and life are inseparable.

We continue to strive for a better world by creating a society that is integrated into our framework.

Hình 1 – Thông tin chung về MegaCorp One trên website của họ

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)?

→ Trả lời:

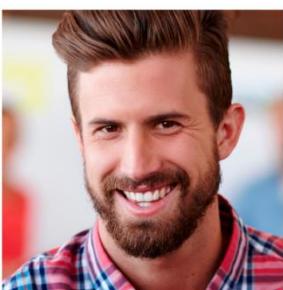
STT	Họ tên	Địa chỉ Email	Chức vụ	Tài khoản MXH
1	Joe Sheer	joe@megacorpone.com	Chief executive officer	@Joe_Sheer
2	Tom Hudson	thudson@megacorpone.com	Web Designer	@TomHudsonMCO
3	Tanya Rivera	trivera@megacorpone.com	Senior Developer	@TanyaRiveraMCO
4	Matt Smith	msmith@megacorpone.com	Marketing Director	@MattSmithMCO

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

Hình 2 – Thông tin về thành viên đang làm việc cho MegaCorp One

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

→ Trả lời: Email của các thành viên thuộc tổ chức đều chứa miền của công ty và có dạng: <địa chỉ>@megacorpone.com hoặc <chữ_cái_đầu_của_tên+họ>@megacorpone.com.

b, Whois Enumeration

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

→ Trả lời: Các name server của MegaCorp One là: NS1.MEGACORPONE.COM, NS2.MEGACORPONE.COM, NS3.MEGACORPONE.COM.

```
(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: 2023-06-13T18:08:24Z
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@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: 2023-10-13T02:00:51Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

Hình 3 – Kết quả trả về khi sử dụng công cụ whois để tìm thông tin về MegaCorp One

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?

→ Trả lời: Không thể sử dụng công cụ whois để tìm kiếm các thông tin của uit.edu.vn.

Khi gõ *whois uit.edu.vn* trên kali thu được kết quả sau:

```
(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
```

Hình 4 – Kết quả trả về khi sử dụng công cụ whois để tìm thông tin về uit.edu.vn

Có thể thấy thông báo không có máy chủ WHOIS cho uit.edu.vn , không có thông tin WHOIS trực tiếp và gợi ý truy cập vào cơ sở dữ liệu WHOIS tại địa chỉ <http://www.vnnic.vn/en>.

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

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

→ Trả lời:

a, Ngày đăng ký tên miền: 02/10/2006.

b, Ngày hết hạn tên miền: 02/10/2024.

c, Chủ sở hữu tên miền: Công ty TNHH PA Việt Nam.

d, Các name server của tên miền: ns1.pavietnam.vn, ns2.pavietnam.vn, nsbak.pavietnam.net.

VNNIC INTERNET RESOURCE WHOIS INFORMATION

This whois query was received from IP Address: 2001:ee0:155:3c48:1d0a:c1da:1f7:a1c1
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

Hình 5 – Kết quả tìm kiếm thông tin về uit.edu.vn trên <http://www.vnnic.vn/en>

c, Google Hacking

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

→ Trả lời: Phó chủ tịch Pháp lý của MegaCorp One là Mike Carlow, email của họ là mcarlow@megacorpone.

Google search results for "vice president of legal of megacorpone". The first result is a LinkedIn profile for Mike Carlow. The second result is a LinkedIn page for 'Contact Us - MegaCorp One' where 'Mike Carlow' is listed.

Hình 6 – Kết quả tìm kiếm vice president of legal of megacorpone trên Google

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?

→ Trả lời:

LinkedIn search results for 'Stan Denvers Collections'. A profile for Stan Denvers is shown, including his email (stan@megacorpone.com) and a 'BEST PROFESSIONAL' badge.

The screenshot shows three search results for 'megacorpone.com'. Each result card contains:

- Sam Hilker** (Sales Associate) located in **Wilmington, NC, US**. Below the card is the URL **1 megacorpone.com**.
- Mutunga Muli** (Electrical Specialist) located in **None**. Below the card is the URL **1 megacorpone.com**.
- Steve Wong** (System Administrator) located in **Vancouver, BC, CA**. Below the card is the URL **1 megacorpone.com**.

Hình 7,8– Kết quả tìm một số nhân viên khác của megacorpone

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

→ Trả lời:

Từ khoá	Ví dụ	Ý nghĩa
site	site:wikipedia.org	Giới hạn kết quả tìm kiếm cho một trang web hoặc một tên miền cụ thể
filetype	filetype:pdf	Tìm kiếm các tệp tin có định dạng cụ thể
inurl	inurl:forum	Tìm kiếm các trang có chứa từ khóa trong URL của trang web.
intext	intext:apple	Tìm kiếm các trang có chứa từ khóa trong nội dung của trang web
intitle	intitle:recipe	Tìm kiếm các trang có chứa từ khóa trong tiêu đề của trang web

Hình 9 – Minh họa cho ví dụ site:wikipedia.org

Hình 10 – Minh họa cho ví dụ filetype:pdf



Google inurl:forum

[uit.edu.vn](https://forum.uit.edu.vn)
https://forum.uit.edu.vn

UIT - Forum: Forums
Việc làm - thực tập. Nơi thông tin về việc làm dành cho SV sắp tốt nghiệp, cơ hội thực tập tại doanh nghiệp. Topics: 6,728 Posts: 14,919. Last Post: VNG ...

[wiktionary.org](https://vi.wiktionary.org/wiki/forum)
https://vi.wiktionary.org/wiki/forum

forum – Wiktionary tiếng Việt
Cuộc hội thảo, hội nghị. Forum sur l'éducation — cuộc hội thảo về giáo dục. (Sử học) Nơi họp chợ (cỗ La Mã). (Sử học) ...

[babla.vn](https://www.babla.vn/tieng-anh-tieng-viet/forum)
https://www.babla.vn/tieng-anh-tieng-viet/forum

FORUM - nghĩa trong tiếng Việt - từ điển bab.la
The publication and its annual forum promote written and face-to-face interdisciplinary discussion around issues in theology and the study of religion.

Hình 11 – Minh họa cho ví dụ inurl:forum

Google intext:apple

[apple.com](https://www.apple.com/vn)
https://www.apple.com/vn

Apple Việt Nam - Trang Web Chính Thức
Mua iPhone 15 Pro, iPhone 15, **Apple** Watch Series 9 và **Apple** Watch Ultra 2 mới ngay. Mua sắm cả Mac, **Apple** TV, iPad, AirPods, phụ kiện và hơn thế nữa. Trả góp lãi suất thấp.

[apple.com](https://www.apple.com/)
https://www.apple.com/ ...

Apple (Việt Nam)
Discover the innovative world of Apple and shop everything iPhone, iPad, Apple Watch, Mac, and Apple TV, plus explore accessories, entertainment, ...

Hình 12 – Minh họa cho ví dụ intext:apple

Google intitle:recipe

[oxfordlearnersdictionaries.com](https://www.oxfordlearnersdictionaries.com)
https://www.oxfordlearnersdictionaries.com/ ...

recipe noun - Definition, pictures, pronunciation and usage ...
. a set of instructions that tells you how to cook something and the ingredients (= items of food) you need for it. recipe for something a recipe for chicken ...

[babla.vn](https://www.babla.vn/tieng-anh-tieng-viet/recipe)
https://www.babla.vn/tieng-anh-tieng-viet/recipe

RECIPE - nghĩa trong tiếng Việt - từ điển bab.la
Nghĩa của "recipe" trong tiếng Việt: công thức nấu ăn · phương pháp · công thức ...

[studytienganhviet.vn](https://www.studytienganhviet.vn/news/andquotorecipe...)
https://www.studytienganhviet.vn/news/andquotorecipe... :

"Recipe" nghĩa là gì: Định Nghĩa, Ví Dụ trong Tiếng Anh
Nghĩa tiếng anh: recipe is a set of instructions telling you how to prepare and cook food, including a list of what food is needed for this. Nghĩa tiếng việt: ...

[merriam-webster.com](https://www.merriam-webster.com)
https://www.merriam-webster.com/rec... :

Recipe Definition & Meaning - Merriam-Webster
5 ngày trước — The meaning of RECIPE is prescription. How to use recipe in a sentence.

Hình 13 – Minh họa cho ví dụ intitle:recipe

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?

→ Trả lời: Khi tìm kiếm thông tin trên **uit.edu.vn** truy cập vào **Tra cứu > Công bố ba công khai** ta thấy thông tin thú vị - **Công khai khảo sát tình hình việc làm đối với sinh viên chính quy**, trong đó sẽ có Danh sách sinh viên tốt nghiệp năm <năm cần tìm>.

Ví dụ xét năm 2019:

**ĐẠI HỌC QUỐC GIA TP.HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ THÔNG TIN**

DANH SÁCH SINH VIÊN PHẦN HỒI NĂM 2019

STT	Mã SV	Đúng ngành đào tạo	Liên quan đến ngành đào tạo	Không liên quan đến ngành đào tạo	Tiếp tục học	Chưa có việc làm	Nhà nước	Tư nhân	Tự tạo việc làm	Các yếu tố nước ngoài	Nơi làm việc (Tỉnh/TP)
1	15520781	x								x	Thành phố Hồ Chí Minh
2	15520988	x						x			Thành phố Hồ Chí Minh
3	14520003				x						Thành phố Hồ Chí Minh
4	14520036	x						x			Tỉnh Tây Ninh
5	14520041				x						Thành phố Hồ Chí Minh
6	14520045	x						x			Thành phố Hồ Chí Minh
7	14520084	x						x			Thành phố Hồ Chí Minh
8	14520117	x						x			Tỉnh Long An

Hình 14 – Một phần danh sách sinh viên phản hồi năm 2019

Chọn MSSV 15520781 và tra trên Google có thể tìm kiếm được một số thông tin liên quan đến sinh viên này:

TT	Mã SV	Họ tên	Lớp	ĐTB	ĐRL	Xếp loại	Số tiền
167	14520950	Trần Văn Tiên	KTMT2014	8.81	87	Giỏi	3,900,000
168	14520004	Hoàng Văn An	KTMT2014	8.73	91	Giỏi	3,900,000
169	14520618	Nguyễn Trọng Nhã	KTMT2014	8.73	82	Giỏi	3,900,000
170	14520232	Trương Quang Giàu	KTMT2014	8.72	100	Giỏi	3,900,000
171	14520734	Nguyễn Hồng Quân	KTMT2014	8.71	94	Giỏi	3,900,000
172	14520555	Nguyễn Thành Nam	KTMT2014	8.69	84	Giỏi	3,900,000
173	14521050	Nguyễn Văn Tuân	KTMT2014	8.62	86	Giỏi	3,900,000
174	14520492	Nguyễn Minh Luân	KTMT2014	8.57	100	Giỏi	3,900,000
175	14520028	Nguyễn Tuấn Anh	KTMT2014	8.47	88	Giỏi	3,900,000
176	15520855	Lữ Khải Thông	KTMT2015	8.9	95	Giỏi	3,900,000
177	15520234	Nguyễn Văn Hiếu	KTMT2015	8.85	80	Giỏi	3,900,000
178	15520146	Lê Vũ Trung Dương	KTMT2015	8.73	93	Giỏi	3,900,000
179	15520781	Nguyễn Quang Thái	KTMT2015	8.63	99	Giỏi	3,900,000

Hình 15 – Một phần danh sách sinh viên nhận học bổng khuyến khích học tập HK1, năm học 2015-2016

d, Netcraft

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

→ Trả lời: Truy cập vào trang web: <https://searchdns.netcraft.com/> > Resources > Research Tools > Site Report.

Trong thanh tìm kiếm nhập <https://www.megacorpone.com/>, thu được các kết quả:

Background

Site title	MegaCorp One - Nanotechnology is the Future	Date first seen	December 2018
Site rank	45824	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English

Network

Site	https://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)	Organisation	MegaCorpOne, Rachel, 89001, United States
IPv4 autonomous systems	AS16276	DNS admin	admin@megacorpone.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Unknown
Reverse DNS	www.megacorpone.com		

IP delegation

IPv4 address (149.56.244.87)

Site Technology (fetched 9 days ago)**Application Servers**

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Apache	Web server software	www.24presse.com , www.smtpcorp.com , www.tutorialspoint.com
Debian	No description	www.hirkereso.hu , www.majorgeeks.com , www.franceso.fr

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	accounts.google.com

Hình 16, 17 – Một số thông tin trả về khi search về megacorpone.com

Nhận thấy, máy chủ ứng dụng đang chạy trên megacorpone.com là Apache.

e, Recon-ng

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

→ Trả lời: Sử dụng recon/domains-hosts/hackertarget để phân giải.

```
[recon-ng][default] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] > modul load recon/domains-hosts/hackertarget
[!] Invalid command: modul load recon/domains-hosts/hackertarget.
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][hackertarget] > info
File Actions Edit View Help
    Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
    Version: 1.1

Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
    Name      Current Value   Required   Description
    SOURCE    default        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
```

Hình 18 – Cài đặt và kiểm tra recon/domains-hosts/hackertarget

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

MEGACORPONE.COM
[*] Country: None
[*] Host: fs1.megacorpone.com
[*] Ip_Address: 51.222.169.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns1.megacorpone.com
[*] Ip_Address: 51.79.37.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: mail2.megacorpone.com
[*] Ip_Address: 51.222.169.213
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

[*] Country: None
[*] Host: ns2.megacorpone.com
[*] Ip_Address: 51.222.39.63
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www2.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns3.megacorpone.com
[*] Ip_Address: 66.70.207.180
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: beta.megacorpone.com
[*] Ip_Address: 51.222.169.209
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	fs1.megacorpone.com	51.222.169.210						hackertarget
2	ns1.megacorpone.com	51.79.37.18						hackertarget
3	mail2.megacorpone.com	51.222.169.213						hackertarget
4	ns2.megacorpone.com	51.222.39.63						hackertarget
5	www2.megacorpone.com	149.56.244.87						hackertarget
6	ns3.megacorpone.com	66.70.207.180						hackertarget
7	beta.megacorpone.com	51.222.169.209						hackertarget
8	syslog.megacorpone.com	51.222.169.217						hackertarget
9	mail.megacorpone.com	51.222.169.212						hackertarget
10	siem.megacorpone.com	51.222.169.215						hackertarget
11	admin.megacorpone.com	51.222.169.208						hackertarget
12	vpn.megacorpone.com	51.222.169.220						hackertarget
13	snmp.megacorpone.com	51.222.169.216						hackertarget
14	router.megacorpone.com	51.222.169.214						hackertarget
15	intranet.megacorpone.com	51.222.169.211						hackertarget
16	support.megacorpone.com	51.222.169.218						hackertarget
17	test.megacorpone.com	51.222.169.219						hackertarget
18	www.megacorpone.com	149.56.244.87						hackertarget

Hình 19,20,21,22,23 – Kết quả thực hiện phân giải tên miền ở hình 20

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	fs1.megacorpone.com	51.222.169.210						hackertarget
2	ns1.megacorpone.com	51.79.37.18						hackertarget
3	mail2.megacorpone.com	51.222.169.213						hackertarget
4	ns2.megacorpone.com	51.222.39.63						hackertarget
5	www2.megacorpone.com	149.56.244.87						hackertarget
6	ns3.megacorpone.com	66.70.207.180						hackertarget
7	beta.megacorpone.com	51.222.169.209						hackertarget
8	syslog.megacorpone.com	51.222.169.217						hackertarget
9	mail.megacorpone.com	51.222.169.212						hackertarget
10	siem.megacorpone.com	51.222.169.215						hackertarget
11	admin.megacorpone.com	51.222.169.208						hackertarget
12	vpn.megacorpone.com	51.222.169.220						hackertarget
13	snmp.megacorpone.com	51.222.169.216						hackertarget
14	router.megacorpone.com	51.222.169.214						hackertarget
15	intranet.megacorpone.com	51.222.169.211						hackertarget
16	support.megacorpone.com	51.222.169.218						hackertarget
17	test.megacorpone.com	51.222.169.219						hackertarget
18	www.megacorpone.com	149.56.244.87						hackertarget

Hình 24 – Xem lịch sử các host

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

→ Trả lời: Tiếp tục sử dụng hackertarget để tìm thông tin về UIT, có 104 host được tìm thấy.

SUMMARY	
[*] 104 total (0 new) hosts found. [recon-ng][default][hackertarget] > show hosts	
19	mx1.uit.edu.vn
20	mapr2022.uit.edu.vn
21	a084742fa316491c8c78564efcbce9e0-68f6236f-vm-80.vlab2.uit.edu.vn
22	host.uit.edu.vn
23	mx2.uit.edu.vn
24	forum.uit.edu.vn
25	sois2017.uit.edu.vn
26	mapr2022.uit.edu.vn
27	vlab.uit.edu.vn
28	mitaka.uit.edu.vn
29	forumbeta.uit.edu.vn
30	inselab.uit.edu.vn
31	api.mmlab.uit.edu.vn
32	annotation.mmlab.uit.edu.vn
33	demo.mmlab.uit.edu.vn
34	vlab.uit.edu.vn
35	519bb137df614dcbeda10e87d53ad8a-0-s-80.vlab.uit.edu.vn
36	console-cloud.vlab.uit.edu.vn
37	qtn.uit.edu.vn
38	iecclub.uit.edu.vn
39	aicub.uit.edu.vn
40	qlhc.uit.edu.vn
41	nc.uit.edu.vn
42	dsc.uit.edu.vn
43	cnsc.uit.edu.vn
44	khtc.uit.edu.vn
45	chungthuc.uit.edu.vn
46	cd.uit.edu.vn
47	tech4covid.uit.edu.vn
48	hcmcovidsafe-h4ovid.uit.edu.vn
49	hcycovid-4-day.tech4covid.uit.edu.vn
50	hcycovid-4-day.tech4covid.uit.edu.vn
51	hcmcovidsafe-gw.tech4covid.uit.edu.vn
52	fce.uit.edu.vn
53	ecommerce.uit.edu.vn
54	khoahocdoit.uit.edu.vn
55	se.uit.edu.vn
56	esetupdate.uit.edu.vn
57	live.uit.edu.vn
58	extensiverading.uit.edu.vn
59	elearning.uit.edu.vn
60	longnghiem.uit.edu.vn
61	sdn.uit.edu.vn
62	tuyensinh.uit.edu.vn
63	auth.uit.edu.vn
64	openstack.uit.edu.vn
65	link.uit.edu.vn
66	notebook.uit.edu.vn
67	dreamsparc.uit.edu.vn
68	portal.uit.edu.vn
69	dbcl.uit.edu.vn
70	phongdl.uit.edu.vn
71	bandl.uit.edu.vn
72	congdoanql.uit.edu.vn
73	acm.uit.edu.vn
74	tracngiem.uit.edu.vn
75	forum.uit.edu.vn
76	debian.uit.edu.vn
77	congdoan.uit.edu.vn
78	khmt.uit.edu.vn
79	lpdn.uit.edu.vn
80	en.uit.edu.vn
81	thuvien.uit.edu.vn
82	www.thuvien.uit.edu.vn
83	cybertrain.uit.edu.vn
84	doantn.uit.edu.vn
85	dangbo.uit.edu.vn
86	huongnghiep.uit.edu.vn
87	oep.uit.edu.vn
88	demodkhp.uit.edu.vn
89	nlp.uit.edu.vn
90	ftp.uit.edu.vn
91	hostmaster.uit.edu.vn
92	mapr.uit.edu.vn
93	sonaas.uit.edu.vn
94	cs.uit.edu.vn
95	aicub.cs.uit.edu.vn
96	service.aicub.cs.uit.edu.vn
97	student.cs.uit.edu.vn
98	banqlcs.uit.edu.vn
99	courses.uit.edu.vn
100	oms.uit.edu.vn
101	netsens.uit.edu.vn
102	photos.uit.edu.vn
103	qldt.uit.edu.vn
104	iot.uit.edu.vn
105	ctgt.uit.edu.vn
106	fit.uit.edu.vn
107	git.uit.edu.vn
108	khmt.uit.edu.vn
109	mmt.uit.edu.vn
110	ktmt.uit.edu.vn
111	student.uit.edu.vn
112	iot.uit.edu.vn
113	appi.iot.uit.edu.vn
114	testbed.iot.uit.edu.vn
115	foimobile.uit.edu.vn
116	iott.uit.edu.vn
117	ecommerce.ittt.uit.edu.vn
118	ptnhtt.uit.edu.vn
119	ctsv.uit.edu.vn
120	www.uit.edu.vn
121	ceday.uit.edu.vn
122	danguy.uit.edu.vn

Hình 25, 26, 27 – 104 host được tìm thấy của uit.edu.vn

f, Open-Source Code

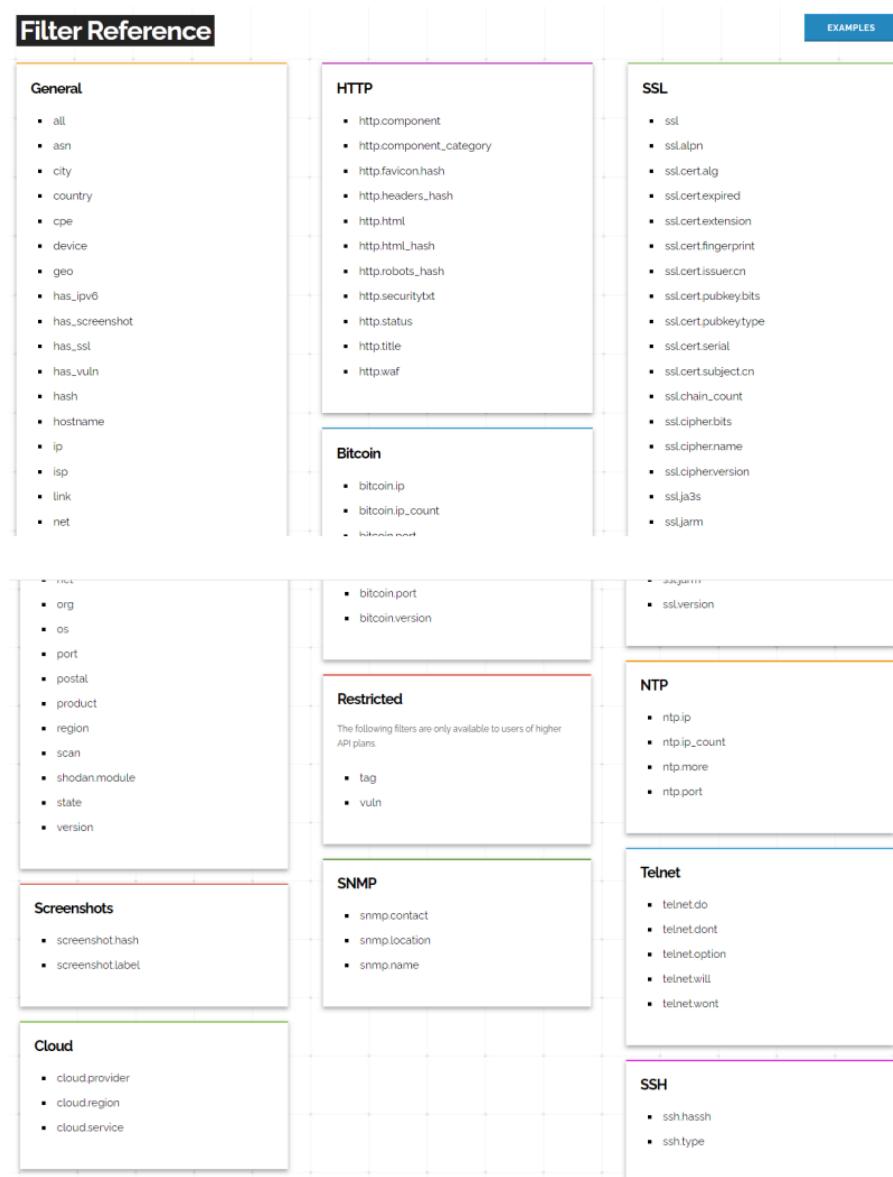
14. Sử dụng 1 trong 2 công cụ Gitrob hoặc Gitleaks để tìm kiếm các thông tin nhạy cảm bị rò rỉ đối với các trường đại học thành viên trong ĐHQG

→ Trả lời: Nhóm bỏ qua câu hỏi cộng điểm này.

g, Shodan

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.

→ Trả lời: Có thể dùng filter để tìm kiếm với cú pháp: **filtername:value**. Ngoài ra, có thể sử dụng “+” hoặc “-“ (AND hoặc OR filter) để kết hợp các filter với nhau.



Hình 28 – Một số filter

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

→ Trả lời:

	Shodan	Search Engine khác
Kết quả tìm kiếm thông thường	Tập trung vào việc tìm kiếm các thiết bị trực tuyến như máy tính, camera, router, webcams, máy chủ, máy in,...	Tập trung vào việc tìm kiếm nội dung trên máy chủ web và các trang web công khai, bao gồm các file, đoạn văn bản, URL và các trang web.
Kết quả tìm kiếm dịch vụ	Cung cấp thông tin về các dịch vụ đang chạy trên các cổng mở, bao gồm các dịch vụ như VPN, VNC và cung cấp thông tin liên quan đến các dịch vụ mà người dùng có thể truy cập được.	Cung cấp kết quả là các sản phẩm liên quan đến dịch vụ (ứng dụng để chạy dịch vụ, document,...).

h, the Harvester

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

→ Trả lời: Khi kiểm tra các source mà công cụ đang có thì không có google nên sẽ tìm kiếm trên các source khác.

Hình 29 – Kết quả kiểm tra phiên bản của theHavester

```

└─# theHarvester -d uit.edu.vn -b bing
*****
* [H][E][A][R][V][E][S][T][E][R] *
* theHarvester 4.4.3
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****
[*] Target: uit.edu.vn
      Searching 0 results.
[*] Searching Bing.
[*] No IPs found.
[*] Emails found: 2
info@uit.edu.vn
phongdaotaodanhuit.edu.vn
[*] Hosts found: 14
daa.uit.edu.vn
drl.uit.edu.vn
dsc.uit.edu.vn
en.uit.edu.vn
fce.uit.edu.vn
forum.uit.edu.vn
is.uit.edu.vn
khmt.uit.edu.vn
nc.uit.edu.vn
portal.uit.edu.vn
se.uit.edu.vn
student.uit.edu.vn
thuvien.uit.edu.vn
tuyensinh.uit.edu.vn

```

Hình 30 – Kết quả tìm kiếm với source bing

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

→ Trả lời: Thực hiện tìm kiếm trên một số nguồn:

```

└─# theHarvester -d uit.edu.vn -b baidu
*****
* [H][E][A][R][V][E][S][T][E][R] *
* theHarvester 4.4.3
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****
[*] Target: uit.edu.vn
[*] Searching Baidu.
[*] No IPs found.
[*] Emails found: 5
19521706@gm.uit.edu.vn
19522499@gm.uit.edu.vn
kietnv@uit.edu.vn
nganlt@uit.edu.vn
sonlt@uit.edu.vn
[*] Hosts found: 3
en.uit.edu.vn
gm.uit.edu.vn
ngochuy.uit.edu.vn

```

Hình 31 – Kết quả tìm kiếm với source baidu

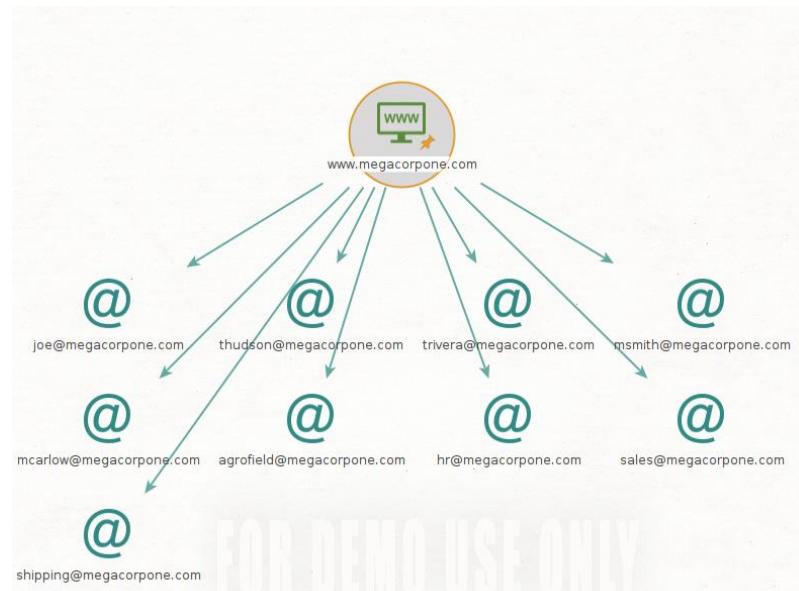
Hình 32,33 – Kết quả tìm kiếm với source baidu

Nhận xét: Sự hiệu quả của mỗi nguồn dữ liệu trong TheHarvester phụ thuộc vào nhiều yếu tố nên không có nguồn nào có thể được xem là tốt hơn một cách tuyệt đối, mà tùy thuộc vào mục tiêu cụ thể và ngữ cảnh sử dụng.

i, Information Gathering Frameworks

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

→ Trả lời: Mở giao diện Meltego > New (để tạo New Graph) > Ở trên thanh Search gõ Web để tìm Website > Kéo icon vào bên trong New Graph > Sửa lại tên web thành www.megacorpone.com > Nhấp chuột phải vào biểu tượng > Chọn All Transforms > Chon Miror: Email address found



Hình 38. Kết quả thực hiện

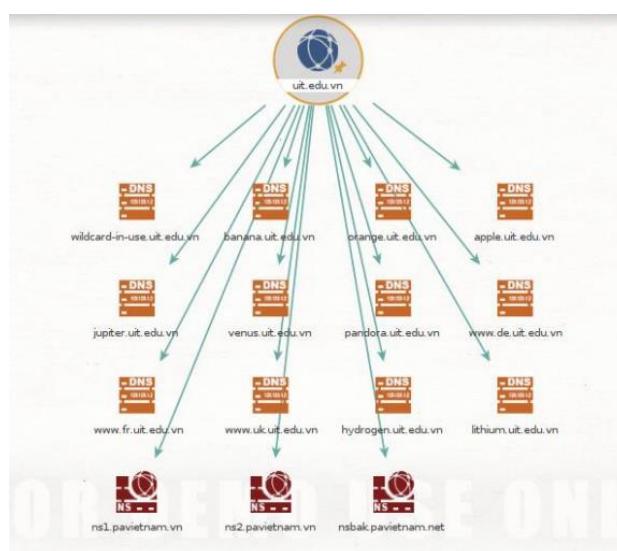
20. Sử dụng công cụ Maltego cho UIT (tên miền: **uit.edu.vn**) và trả lời các câu hỏi sau:

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

→ Trả lời:

a, Các bản ghi DNS của uit.edu.vn

Từ giao diện Maltego > New Graph > Search Domain và đưa ra > Sửa domain mặc định thành uit.edu.vn > Chuột phải vào biểu tượng > All Transforms > Chọn To Domain và To DNS Name – Name Server.



Hình 39. Các bản ghi DNS

b, Các website và địa chỉ tương ứng của uit.edu.vn

Thực hiện tương tự, ở All Transforms > Chọn To website using domain.



Hình 40. Các website và địa chỉ tương ứng

2. THU THẬP THÔNG TIN CHỦ ĐỘNG

j, DNS Enumeration

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

→ Trả lời: SOA, SRV, ASFDB, DCHID, HIP

Một số ví dụ cho bản ghi DNS:

```

(kali㉿kali)-[~]
└─$ host -t NS megacorpone.com
megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns3.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.

(kali㉿kali)-[~]
└─$ host -t A megacorpone.com
megacorpone.com has no A record

(kali㉿kali)-[~]
└─$ host -t MX megacorpone.com
megacorpone.com mail is handled by 50 mail.megacorpone.com.
megacorpone.com mail is handled by 60 mail2.megacorpone.com.
megacorpone.com mail is handled by 10 fb.mail.gandi.net.
megacorpone.com mail is handled by 20 spool.mail.gandi.net.

(kali㉿kali)-[~]
└─$ host -t PTR megacorpone.com
megacorpone.com has no PTR record

(kali㉿kali)-[~]
└─$ host -t CNAME megacorpone.com
megacorpone.com has no CNAME record

(kali㉿kali)-[~]
└─$ host -t TXT megacorpone.com
megacorpone.com descriptive text "Try Harder"
megacorpone.com descriptive text "google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXFCJ32hMNV3GtC0wWq5pA"
  
```

Hình 41. Các bản ghi DNS (NS, A, MX, PTR, CNAME, TXT) của megacorpone.com

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

→ Trả lời:

```
(kali㉿kali)-[~]
└─$ host -t txt uit.edu.vn
uit.edu.vn descriptive text "google-site-verification=wjArKGa37oHK083XqT2C91tPny8NLttGS0aU5pjKiY"
uit.edu.vn descriptive text "MS=E431E3CA3EFF5A6431E2378C924984A8A0334ABC"
uit.edu.vn descriptive text "svp60rjlwr6s19rn9t013cfwm3xmqx7h"
uit.edu.vn descriptive text "sqmby27vn74pm290pl0fq4hcr08gst5r"
uit.edu.vn descriptive text "v=spf1 include:_spf.google.com ~all"

(kali㉿kali)-[~]
└─$ host -t mx uit.edu.vn
uit.edu.vn mail is handled by 10 aspmx.l.google.com.
uit.edu.vn mail is handled by 40 aspmx3.googlemail.com.
uit.edu.vn mail is handled by 40 aspmx2.googlemail.com.
uit.edu.vn mail is handled by 20 alt2.aspmx.l.google.com.
uit.edu.vn mail is handled by 20 alt1.aspmx.l.google.com.
```

Hình 41. Các bản ghi DNS (TXT, MX) của uit.edu.vn

23. 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?

→ Trả lời: Nhận thấy, các địa chỉ trả về đều giống nhau. Cấu hình DNS của tên miền uit.edu.vn có sử dụng wildcard * nên nếu xảy ra trường hợp một DNS query nào đó không có hostname thì sẽ được gắn với wildcard * trả về cùng một IP.

```
(kali㉿kali)-[~]
└─$ host uit.edu.vn
uit.edu.vn has address 118.69.123.140
uit.edu.vn mail is handled by 10 aspmx.l.google.com.
uit.edu.vn mail is handled by 40 aspmx2.googlemail.com.
uit.edu.vn mail is handled by 20 alt2.aspmx.l.google.com.
uit.edu.vn mail is handled by 40 aspmx3.googlemail.com.
uit.edu.vn mail is handled by 20 alt1.aspmx.l.google.com.

(kali㉿kali)-[~]
└─$ 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

(kali㉿kali)-[~]
└─$ 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)-[~]
└─$ 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
```

Hình 43. Kết quả trả về của các host không tồn tại trong uit.edu.vn

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

→ Trả lời: Sử dụng wordlist Seclist

<https://github.com/danielmiessler/SecLists/blob/285474cf9bff85f3323c5a1ae436f7>

8acd1cb62c/Discovery/DNS/subdomains-top1million-5000.txt

```
(tmai@LAPTOP-EPF3I2KM) [~]
$ for name in $(cat wordlist.txt); do host $name.megacorpone.com; done | grep -v 'not found'
www.megacorpone.com has address 149.56.244.87
mail.megacorpone.com has address 51.222.169.212
ftp.megacorpone.com has address 125.235.4.59
localhost.megacorpone.com has address 125.235.4.59
webmail.megacorpone.com has address 125.235.4.59
smtp.megacorpone.com has address 125.235.4.59
webdisk.megacorpone.com has address 125.235.4.59
pop.megacorpone.com has address 125.235.4.59
cpanel.megacorpone.com has address 125.235.4.59
whm.megacorpone.com has address 125.235.4.59
ns1.megacorpone.com has address 51.79.37.18
ns2.megacorpone.com has address 51.222.39.63
```

Hình 44. Các hostname hợp lệ khác của megacorpone.com

25. 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.

→ Trả lời:

- file bashscript.sh

```
#!/bin/bash
domains=("hcmus.edu.vn" "hcmussh.edu.vn" "uit.edu.vn" "hcmut.edu.vn" "uel.edu.vn" "hcmier.edu.vn" "vnuhcm.edu.vn")
for domain in ${domains[@]}; do
echo "- Domain: $domain"
for nameServer in `host -t ns $domain 2>/dev/null | cut -d " " -f 4`; do
echo "+ Nameserver: $nameServer"
echo "~~~Zone transfer..."
host -l $domain $nameServer 2>/dev/null
echo
echo -----
done
echo
echo "*****"
echo
done
```

Hình 45. Nội dung file bashscript.sh

- ./bashscript.sh

```
(tmai@LAPTOP-EPF3I2KM)-[~]
$ ./bashscript.sh
- Domain: hcmus.edu.vn
+ Nameserver: dns1.hcmus.edu.vn.
~~~Zone transfer...
;; Connection to 14.241.254.131#53(14.241.254.131) for hcmus.edu.vn failed: timed out.
;; Connection to 14.241.254.131#53(14.241.254.131) for hcmus.edu.vn failed: timed out.
;; Connection to 64:ff9b::ef1:fe83#53(64:ff9b::ef1:fe83) for hcmus.edu.vn failed: network unreachable.

-----
+ Nameserver: dns2.hcmus.edu.vn.
~~~Zone transfer...
;; Connection to 115.73.217.121#53(115.73.217.121) for hcmus.edu.vn failed: timed out.
;; Connection to 115.73.217.121#53(115.73.217.121) for hcmus.edu.vn failed: timed out.
;; Connection to 64:ff9b::7349:d979#53(64:ff9b::7349:d979) for hcmus.edu.vn failed: network unreachable.

-----
+ Nameserver: server.hcmus.edu.vn.
~~~Zone transfer...
Using domain server:
Name: server.hcmus.edu.vn.
Address: 171.244.202.180#53
Aliases:

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

-----
*****
```

```
- Domain: hcmussh.edu.vn
+ Nameserver: server.vnuhcm.edu.vn.
~~~Zone transfer...
Using domain server:
Name: server.vnuhcm.edu.vn.
Address: 103.88.121.201#53
Aliases:

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

-----
+ Nameserver: vnuserserv.vnuhcm.edu.vn.
~~~Zone transfer...
Using domain server:
Name: vnuserserv.vnuhcm.edu.vn.
Address: 103.88.121.200#53
Aliases:

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

-----
*****
```

```
- Domain: uit.edu.vn
+ Nameserver: ns2.pavietnam.vn.
~~~Zone transfer...
Using domain server:
Name: ns2.pavietnam.vn.
Address: 222.255.121.247#53
Aliases:

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

-----
+ Nameserver: nsbak.pavietnam.net.
~~~Zone transfer...
Using domain server:
Name: nsbak.pavietnam.net.
Address: 112.213.89.22#53
Aliases:

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

-----
+ Nameserver: ns1.pavietnam.vn.
~~~Zone transfer...
Using domain server:
Name: ns1.pavietnam.vn.
Address: 112.213.89.3#53
Aliases:

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

-----
*****
```

```
- Domain: hcmut.edu.vn
+ Nameserver: dns1.hcmut.edu.vn.
~~~Zone transfer...
Using domain server:
Name: dns1.hcmut.edu.vn.
Address: 101.99.31.218#53
Aliases:

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

-----
+ Nameserver: dns2.hcmut.edu.vn.
~~~Zone transfer...
Using domain server:
Name: dns2.hcmut.edu.vn.
Address: 221.133.13.115#53
Aliases:

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

-----
+ Nameserver: dns3.hcmut.edu.vn.
~~~Zone transfer...
Using domain server:
Name: dns3.hcmut.edu.vn.
Address: 203.205.32.235#53
Aliases:

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

-----
+ Nameserver: dns4.hcmut.edu.vn.
~~~Zone transfer...
;; Connection to 203.205.32.236#53(203.205.32.236) for hcmut.edu.vn failed: timed out.
;; Connection to 203.205.32.236#53(203.205.32.236) for hcmut.edu.vn failed: timed out.
;; Connection to 64:ff9b::cbc0:20ec#53(64:ff9b::cbc0:20ec) for hcmut.edu.vn failed: network unreachable.

-----
*****
```

```

- Domain: uel.edu.vn
+ Nameserver: ns1.dns.net.vn.
~~~Zone transfer...
Using domain server:
Name: ns1.dns.net.vn.
Address: 210.211.108.160#53
Aliases:

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

-----
+ Nameserver: ns2.dns.net.vn.
~~~Zone transfer...
Using domain server:
Name: ns2.dns.net.vn.
Address: 103.45.229.100#53
Aliases:

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

```

```

- Domain: hcmier.edu.vn
+ Nameserver: server.vnuhcm.edu.vn.
~~~Zone transfer...
Using domain server:
Name: server.vnuhcm.edu.vn.
Address: 103.88.121.201#53
Aliases:

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

-----
+ Nameserver: vnuserv.vnuhcm.edu.vn.
~~~Zone transfer...
Using domain server:
Name: vnuserv.vnuhcm.edu.vn.
Address: 103.88.121.200#53
Aliases:

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

```

```

- Domain: vnuhcm.edu.vn
+ Nameserver: vnuserv.vnuhcm.edu.vn.
~~~Zone transfer...
Using domain server:
Name: vnuserv.vnuhcm.edu.vn.
Address: 103.88.121.200#53
Aliases:

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

-----
+ Nameserver: ns2.vdc2.vn.
~~~Zone transfer...
Using domain server:
Name: ns2.vdc2.vn.
Address: 14.225.232.26#53
Aliases:

vnuhcm.edu.vn has address 103.88.121.29
vnuhcm.edu.vn name server vnuserv.vnuhcm.edu.vn.
vnuhcm.edu.vn name server server.vnuhcm.edu.vn.
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
baixecktx.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.cntttt.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
cps.vnuhcm.edu.vn has address 112.78.11.146
ct.vnuhcm.edu.vn has address 203.162.147.252
data.vnuhcm.edu.vn has address 203.162.147.185
dataonline.vnuhcm.edu.vn has address 203.162.44.60
demo.vnuhcm.edu.vn has address 103.88.121.29
demo-cloud.vnuhcm.edu.vn has address 103.88.121.64
demo-khcn.vnuhcm.edu.vn has address 203.162.147.185
demo-lms.vnuhcm.edu.vn has address 103.88.121.142
demo-portal.vnuhcm.edu.vn has address 203.128.241.215
demo-portal-admin.vnuhcm.edu.vn has address 203.128.241.215
demo-portal-static.vnuhcm.edu.vn has address 203.128.241.21
demo1.vnuhcm.edu.vn has address 203.162.147.185
demotuyensinh.vnuhcm.edu.vn has address 203.162.147.186
doancoquan.vnuhcm.edu.vn has address 203.162.147.186
doancoquan.vnuhcm.edu.vn has address 103.74.123.10
doantn.vnuhcm.edu.vn has address 203.162.44.83
email-reply.vnuhcm.edu.vn has address 103.88.121.53
gddhhoinhapquocte.vnuhcm.edu.vn has address 123.30.191.189
greeting-card.vnuhcm.edu.vn has address 203.162.147.185
hoidong.vnuhcm.edu.vn has address 203.162.147.185
hoithaocokhi.vnuhcm.edu.vn has address 165.22.97.200
hoithaogiaothong.vnuhcm.edu.vn has address 206.189.35.164
hosting.vnuhcm.edu.vn has address 203.162.147.185
hotrokythuat.vnuhcm.edu.vn has address 112.78.11.146
idm.vnuhcm.edu.vn has address 103.88.123.51
it-support.vnuhcm.edu.vn has address 112.78.11.146
jobs.vnuhcm.edu.vn has address 103.88.123.54
khaosat.vnuhcm.edu.vn has address 203.162.147.185

```

```

khcn.vnuhcm.edu.vn has address 203.162.147.185
quanly.khcn.vnuhcm.edu.vn has address 118.69.123.142
khcn2018.vnuhcm.edu.vn has address 103.88.121.35
khoanhkhaodothidaihoc.vnuhcm.edu.vn has address 123.30.78.232
kitucxa.vnuhcm.edu.vn has address 45.117.77.102
ksknsvtn.vnuhcm.edu.vn has address 203.162.44.60
ktx.vnuhcm.edu.vn has address 45.117.77.103
mail.ktx.vnuhcm.edu.vn has address 203.162.44.60
ktxdhqg.vnuhcm.edu.vn has address 45.117.77.102
ktxdhqghcm.vnuhcm.edu.vn has address 123.30.236.140
lichtuan.vnuhcm.edu.vn has address 203.162.147.195
live.vnuhcm.edu.vn has address 42.116.11.16
manage-01.vnuhcm.edu.vn has address 103.88.123.64
manage-02.vnuhcm.edu.vn has address 103.88.121.41
meeting.vnuhcm.edu.vn has address 203.162.147.247
noc.vnuhcm.edu.vn has address 112.78.10.40
ns.vnuhcm.edu.vn has address 14.225.232.25
ns1.vnuhcm.edu.vn has address 14.225.232.25
ns2.vnuhcm.edu.vn has address 14.225.232.25
ntb.vnuhcm.edu.vn has address 103.88.88.88
phapluat.vnuhcm.edu.vn has address 74.86.148.43
portal-st.vnuhcm.edu.vn has address 103.88.121.38
qlcb.vnuhcm.edu.vn has address 118.69.123.137
qlda-vp.vnuhcm.edu.vn has address 103.88.121.138
qlda-xd.vnuhcm.edu.vn has address 103.88.121.137
qldt.vnuhcm.edu.vn has address 103.88.121.38
qtmvp.vnuhcm.edu.vn has address 203.163.1.150

```

```

quanlydetai.vnuhcm.edu.vn has address 115.78.164.32
rankingdata.vnuhcm.edu.vn has address 103.88.121.33
rk.vnuhcm.edu.vn has address 103.88.121.33
rkd.vnuhcm.edu.vn has address 103.88.121.33
rm.vnuhcm.edu.vn has address 103.88.121.37
rnm.vnuhcm.edu.vn has address 103.88.121.37
server.vnuhcm.edu.vn has address 103.88.121.201
server.vnuhcm.edu.vn has address 14.225.232.25
server3.vnuhcm.edu.vn has address 203.162.147.149
sm-vnu.vnuhcm.edu.vn has address 203.162.44.47
static.vnuhcm.edu.vn has address 103.88.121.29
svktx.vnuhcm.edu.vn has address 45.117.77.102
tapchikhoahoc.vnuhcm.edu.vn has address 203.162.147.185
tchc.vnuhcm.edu.vn has address 203.162.147.241
test.vnuhcm.edu.vn has address 203.162.147.186
testbed.vnuhcm.edu.vn has address 203.162.44.55
testing.vnuhcm.edu.vn has address 203.162.147.179
testweb.vnuhcm.edu.vn has address 123.30.78.233
thinangluc.vnuhcm.edu.vn has address 118.69.123.136
thinangluc.vnuhcm.edu.vn has address 45.122.249.72
thinangluc-test.vnuhcm.edu.vn has address 221.133.13.124
thumoi.vnuhcm.edu.vn has address 125.253.116.180
thuongnien.vnuhcm.edu.vn has address 203.162.147.252
tspl.vnuhcm.edu.vn has address 203.162.44.60
ttgdqpm.vnuhcm.edu.vn has address 222.255.69.250
ttqlptkdt.vnuhcm.edu.vn has address 203.162.44.60
ttqlptkdt-beta.vnuhcm.edu.vn has address 203.162.44.60
ttddtt.vnuhcm.edu.vn has address 103.88.123.130
tuoitre.vnuhcm.edu.vn has address 210.211.118.168
tuvantuyensinh.vnuhcm.edu.vn has address 203.162.147.185
dangky.tuyensinh.vnuhcm.edu.vn has address 203.162.147.196
vc.vnuhcm.edu.vn has address 171.244.28.100
vnu-f.vnuhcm.edu.vn has address 103.88.121.141
www.vnu-f.vnuhcm.edu.vn has address 103.88.121.141
vnu-f2.vnuhcm.edu.vn has address 103.88.123.5
vnu20.vnuhcm.edu.vn has address 203.162.147.185

```

```

vnuc.vnuhcm.edu.vn has address 112.78.11.146
vnuserv.vnuhcm.edu.vn has address 103.88.121.200
vnuserv.vnuhcm.edu.vn has address 14.225.232.25
voice.vnuhcm.edu.vn has address 203.162.147.187
wifi.vnuhcm.edu.vn has address 10.238.239.1
www.vnuhcm.edu.vn has address 103.88.121.29
-----
```

```

+ Nameserver: ns1.vdc2.vn.
~~~Zone transfer...
Using domain server:
Name: ns1.vdc2.vn.
Address: 14.225.232.25#53
Aliases:

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

```

-----
```

```

+ Nameserver: server.vnuhcm.edu.vn.
~~~Zone transfer...
Using domain server:
Name: server.vnuhcm.edu.vn.
Address: 103.88.121.201#53
Aliases:

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

```

*****
```

Hình 46-56. Kết quả trả về khi thực thi file

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

→ Trả lời: Sử dụng lệnh dnsrecon --help

```
-t TYPE, --type TYPE Type of enumeration to perform.
Possible types:
    std:      SOA, NS, A, AAAA, MX and SRV.
    rvl:      Reverse lookup of a given CIDR or IP range.
    brt:      Brute force domains and hosts using a given dictionary.
    srv:      SRV records.
    axfr:     Test all NS servers for a zone transfer.
    bing:     Perform Bing search for subdomains and hosts.
    yand:     Perform Yandex search for subdomains and hosts.
    crt:      Perform crt.sh search for subdomains and hosts.
    snoop:    Perform cache snooping against all NS servers for a given domain, testing
              all with file containing the domains, file given with -D option.

    tld:      Remove the TLD of given domain and test against all TLDs registered in IANA.
    zonewalk: Perform a DNSSEC zone walk using NSEC records.
```

Hình 57. Danh sách các loại enumeration có thể được sử dụng cùng tùy chọn -t

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

→ Trả lời:

- VD1: Filter out of brute force domain lookup, records that resolve to the wildcard defined IP address when saving records.

+ Sử dụng lệnh dnsrecon -d megacorpone.com -f

```
[tmai@LAPTOP-EPF3I2KM] ~
$ dnsrecon -d megacorpone.com -f
[*] 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
[*]   Bind Version for 66.70.207.180 "9.11.5-P4-5.1+deb10u2-Debian"
[*]   NS ns1.megacorpone.com 51.79.37.18
[*]   Bind Version for 51.79.37.18 "9.11.5-P4-5.1+deb10u2-Debian"
[*]   NS ns2.megacorpone.com 51.222.39.63
[*]   Bind Version for 51.222.39.63 "9.11.5-P4-5.1+deb10u2-Debian"
[*]   MX mail.megacorpone.com 51.222.169.212
[*]   MX spool.mail.gandi.net 217.70.178.1
[*]   MX mail2.megacorpone.com 51.222.169.213
[*]   MX fb.mail.gandi.net 217.70.178.217
[*]   MX fb.mail.gandi.net 217.70.178.215
[*]   MX fb.mail.gandi.net 217.70.178.216
[*]   MX spool.mail.gandi.net 2001:4b98:e00::1
[*]   MX fb.mail.gandi.net 2001:4b98:dc4:8::215
[*]   MX fb.mail.gandi.net 2001:4b98:dc4:8::216
[*]   MX fb.mail.gandi.net 2001:4b98:dc4:8::217
[*]   TXT megacorpone.com google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNv3GtC0wWq5pA
[*]   TXT megacorpone.com Try Harder
[*] Enumerating SRV Records
[-] No SRV Records Found for megacorpone.com
```

Hình 58. Ví dụ 1

- VD2: Perform Bing enumeration with standard enumeration

- Sử dụng lệnh dnsrecon -d megacorpone.com -b

```
(tmai@LAPTOP-EPF3I2KM) [~]
$ dnsrecon -d megacorpone.com -b
[*] 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
[*] Bind Version for 66.70.207.180 "9.11.5-P4-5.1+deb10u2-Debian"
[*] NS ns1.megacorpone.com 51.79.37.18
[*] Bind Version for 51.79.37.18 "9.11.5-P4-5.1+deb10u2-Debian"
[*] NS ns2.megacorpone.com 51.222.39.63
[*] Bind Version for 51.222.39.63 "9.11.5-P4-5.1+deb10u2-Debian"
[*] MX mail.megacorpone.com 51.222.169.212
[*] MX spool.mail.gandi.net 217.70.178.1
[*] MX mail2.megacorpone.com 51.222.169.213
[*] MX fb.mail.gandi.net 217.70.178.215
[*] MX fb.mail.gandi.net 217.70.178.216
[*] MX fb.mail.gandi.net 217.70.178.217
[*] MX spool.mail.gandi.net 2001:4b98:e00::1
[*] MX fb.mail.gandi.net 2001:4b98:dc4:8::217
[*] MX fb.mail.gandi.net 2001:4b98:dc4:8::216
[*] MX fb.mail.gandi.net 2001:4b98:dc4:8::215
[*] TXT megacorpone.com google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXFCJ32hMNV3GtC0wWq5pA
[*] TXT megacorpone.com Try Harder
[*] Enumerating SRV Records
[-] No SRV Records Found for megacorpone.com
[*] Performing Bing Search Enumeration
[*] A 3Amegacorpone.com 125.235.4.59
[*] A 3megacorpone.com 125.235.4.59
[*] A 253amegacorpone.com 125.235.4.59
[+] 3 Records Found
```

Hình 59. Ví dụ 2

28. 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?

→ Trả lời:

DNSEnum	DNSRecon
<ul style="list-style-type: none"> - Khó sử dụng hơn DNSRecon, yêu cầu một số cấu hình. - Khá chính xác, độ chính xác phụ thuộc vào các yêu cầu/ nhiệm vụ cụ thể và nguồn dữ liệu. - Thường cung cấp kết quả dưới dạng văn bản thuần tuý. - Số lượng kết quả phụ thuộc vào các tùy chọn và nhiệm vụ cụ thể đã chọn 	<ul style="list-style-type: none"> - Đơn giản, dễ sử dụng. - Độ chính xác cao, đáng tin cậy. - Cung cấp kết quả dưới dạng bảng cho nhiều loại bản ghi DNS khác nhau. - Kết quả phụ thuộc vào tên miền mục tiêu và cơ sở hạ tầng DNS.

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

→ Trả lời:

- nmap scan report 192.168.23.129

```
(tmai@LAPTOP-EPF3I2KM) ~]$ sudo nmap -sS 192.168.23.129
[sudo] password for tmai:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:32 +07
Nmap scan report for 192.168.23.129 (192.168.23.129)
Host is up (0.0040s 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

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

Hình 60. Kết quả thực hiện câu lệnh scan

- 3 gói tin wireshark [SYN],[SYN,ACK],[RST,ACK]

46 0.166699383 172.18.144.89	192.168.23.129	TCP	58 61084 - 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47 0.166616245 172.18.144.89	192.168.23.129	TCP	58 61084 - 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48 0.166623243 172.18.144.89	192.168.23.129	TCP	58 61084 - 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49 0.166639888 172.18.144.89	192.168.23.129	TCP	58 61084 - 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
50 0.166637690 172.18.144.89	192.168.23.129	TCP	58 61084 - 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51 0.166644569 172.18.144.89	192.168.23.129	TCP	58 61084 - 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52 0.166651458 172.18.144.89	192.168.23.129	TCP	58 61084 - 5099 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53 0.166658545 172.18.144.89	192.168.23.129	TCP	58 61084 - 1309 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54 0.166665288 172.18.144.89	192.168.23.129	TCP	58 61084 - 1309 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55 0.166672211 172.18.144.89	192.168.23.129	TCP	58 61084 - 14090 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
56 0.171936875 192.168.23.129	172.18.144.89	TCP	54 993 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57 0.171937184 192.168.23.129	172.18.144.89	TCP	54 1720 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58 0.171948361 192.168.23.129	172.18.144.89	TCP	54 1025 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 0.171948361 192.168.23.129	172.18.144.89	TCP	54 199 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60 0.171948476 192.168.23.129	172.18.144.89	TCP	54 8080 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 0.171996631 192.168.23.129	172.18.144.89	TCP	54 255 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62 0.172006631 192.168.23.129	172.18.144.89	TCP	54 1389 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 0.172006638 192.168.23.129	172.18.144.89	TCP	54 1389 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64 0.172614440 192.168.23.129	172.18.144.89	TCP	54 14000 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 0.172614461 192.168.23.129	172.18.144.89	TCP	54 8888 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
66 0.172613897 192.168.23.129	172.18.144.89	TCP	58 5999 - 61084 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
67 0.172683692 172.18.144.89	192.168.23.129	TCP	54 61084 - 5999 [RST] Seq=1 Win=0 Len=0
68 0.172106743 192.168.23.129	172.18.144.89	TCP	58 445 - 61084 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
69 0.172159141 192.168.23.129	172.18.144.89	TCP	58 80 - 61084 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
70 0.172174021 192.168.23.129	172.18.144.89	TCP	58 139 - 61084 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
71 0.172159379 192.168.23.129	172.18.144.89	TCP	54 999 - 61084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
72 0.172107026 192.168.23.129	172.18.144.89	TCP	54 135 - 61084 [RST, ACK] Seq=3 Ack=1 Win=0 Len=0
73 0.172107026 192.168.23.129	172.18.144.89	TCP	54 53 - 61084 [RST, ACK] Seq=3 Ack=1 Win=0 Len=0
74 0.172107132 192.168.23.129	172.18.144.89	TCP	54 53 - 61084 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
75 0.172197393 172.18.144.89	192.168.23.129	TCP	54 61084 - 80 [RST] Seq=1 Win=0 Len=0
76 0.172199781 172.18.144.89	192.168.23.129	TCP	54 61084 - 445 [RST] Seq=1 Win=0 Len=0
77 0.172201953 172.18.144.89	192.168.23.129	TCP	54 61084 - 139 [RST] Seq=1 Win=0 Len=0
78 0.172208745 172.18.144.89	192.168.23.129	TCP	54 61084 - 53 [RST] Seq=1 Win=0 Len=0

Hình 61. Kết quả bắt gói tin [SYN],[SYN,ACK],[RST,ACK]

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

→ Trả lời:

- nmap scan report 192.168.23.129

```
[tmai@LAPTOP-EPP3I2KM] ~]
$ sudo nmap -sT 192.168.23.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:41 +07
Nmap scan report for 192.168.23.129 (192.168.23.129)
Host is up (0.52s 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

Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
```

Hình 62. Kết quả thực hiện câu lệnh scan

- 3 gói tin wireshark [SYN],[SYN,ACK],[RST,ACK]

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000018167	172.18.144.89	192.168.23.129	TCP	58	43048 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000037282	172.18.144.89	192.168.23.129	TCP	54	43048 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
5	0.001104717	192.168.23.129	172.18.144.89	TCP	54	89 → 43048 [RST] Seq=1 Win=0 Len=0
L	7 0.001104831	192.168.23.129	172.18.144.89	TCP	54	443 → 43048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	0.133677610	172.18.144.89	192.168.23.129	TCP	74	49474 → 59090 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
13	0.133709380	172.18.144.89	192.168.23.129	TCP	74	52124 → 139 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
14	0.1337124732	172.18.144.89	192.168.23.129	TCP	74	36754 → 3306 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
15	0.1337130415	172.18.144.89	192.168.23.129	TCP	74	34020 → 120 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
16	0.133758098	172.18.144.89	192.168.23.129	TCP	74	40718 → 441 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
17	0.133769229	172.18.144.89	192.168.23.129	TCP	74	35464 → 22 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
18	0.133782281	172.18.144.89	192.168.23.129	TCP	74	47526 → 23 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
19	0.133798310	172.18.144.89	192.168.23.129	TCP	74	58728 → 88 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
20	0.133813749	172.18.144.89	192.168.23.129	TCP	74	55998 → 113 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
21	0.133825587	172.18.144.89	192.168.23.129	TCP	74	3806 → 143 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310186 Tscr=0 WS=128
22	0.133702245	192.168.23.129	172.18.144.89	TCP	74	5900 → 49474 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=2525310186 WS=128
23	0.133702245	192.168.23.129	172.18.144.89	TCP	74	23 → 47526 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=2525310186 WS=128
24	0.137022583	192.168.23.129	172.18.144.89	TCP	54	143 → 34818 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.137086953	192.168.23.129	172.18.144.89	TCP	54	113 → 55998 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.137107943	192.168.23.129	172.18.144.89	TCP	74	88 → 58720 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=2525310186 WS=32
27	0.137116810	192.168.23.129	172.18.144.89	TCP	54	135 → 52120 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
28	0.137120937	172.18.144.89	192.168.23.129	TCP	66	49474 → 59090 [ACK] Seq=1 Ack=1 Win=64896 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=2525310186 WS=32
29	0.137120937	172.18.144.89	192.168.23.129	TCP	66	49474 → 59090 [ACK] Seq=1 Ack=1 Win=64896 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=2525310186 WS=32
30	0.137129523	192.168.23.129	172.18.144.89	TCP	74	445 → 35464 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=2525310186 WS=32
31	0.137129923	192.168.23.129	172.18.144.89	TCP	54	143 → 38964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	0.137136922	172.18.144.89	192.168.23.129	TCP	66	47526 → 23 [ACK] Seq=1 Ack=1 Win=64896 Len=0 Tsv=2525310189 Tscr=113033
33	0.137146854	172.18.144.89	192.168.23.129	TCP	66	58720 → 89 [ACK] Seq=1 Ack=1 Win=64896 Len=0 Tsv=2525310189 Tscr=113033
34	0.137146862	172.18.144.89	192.168.23.129	TCP	66	36754 → 3306 [ACK] Seq=1 Ack=1 Win=64896 Len=0 Tsv=2525310189 Tscr=113033
35	0.137158707	192.168.23.129	172.18.144.89	TCP	74	22 → 35464 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=2525310186 WS=32
36	0.137169986	172.18.144.89	192.168.23.129	TCP	66	48710 → 449 [ACK] Seq=1 Ack=1 Win=64896 Len=0 Tsv=2525310189 Tscr=113033
37	0.137166294	172.18.144.89	192.168.23.129	TCP	66	35464 → 22 [ACK] Seq=1 Ack=1 Win=64896 Len=0 Tsv=2525310189 Tscr=113033
38	0.137266854	172.18.144.89	192.168.23.129	TCP	66	49474 → 59090 [ACK] Seq=1 Ack=1 Win=64896 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=113033
39	0.137266854	172.18.144.89	192.168.23.129	TCP	66	36754 → 3306 [ACK] Seq=1 Ack=1 Win=64896 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=113033
40	0.137288560	172.18.144.89	192.168.23.129	TCP	66	48710 → 449 [RST, ACK] Seq=1 Ack=1 Win=64896 Len=0 MSS=1460 SACK_PERM Tsv=113033 Tscr=113033
41	0.137302232	172.18.144.89	192.168.23.129	TCP	66	35464 → 22 [RST, ACK] Seq=1 Ack=1 Win=64896 Len=0 Tsv=2525310189 Tscr=113033
42	0.137314848	172.18.144.89	192.168.23.129	TCP	66	47526 → 23 [RST, ACK] Seq=1 Ack=1 Win=64896 Len=0 Tsv=2525310189 Tscr=113033
43	0.137326208	172.18.144.89	192.168.23.129	TCP	66	58720 → 89 [RST, ACK] Seq=1 Ack=1 Win=64896 Len=0 Tsv=2525310189 Tscr=113033
44	0.137396574	172.18.144.89	192.168.23.129	TCP	74	41478 → 1025 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310189 Tscr=0 WS=128
45	0.137426184	172.18.144.89	192.168.23.129	TCP	74	41002 → 116 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310189 Tscr=0 WS=128
46	0.137450219	172.18.144.89	192.168.23.129	TCP	74	52458 → 443 [SYN] Seq=0 Win=64860 Len=0 MSS=1410 SACK_PERM Tsv=2525310189 Tscr=0 WS=128

Hình 63. Kết quả bắt gói tin [SYN],[SYN,ACK],[RST,ACK]

31. 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...)

→ Trả lời:

SYN Scan	TCP Connect Scan
- Thời gian quét nhanh.	- Thời gian quét lâu hơn (lâu hơn SYN Scan).
- Số lượng gói tin gửi đi ít hơn.	- Số lượng gói tin gửi đi lớn.

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

→ Trả lời:

- Thực thi file task32.sh:

```
(tmai@LAPTOP-EPF3I2KM) ~
$ cat task32.sh
#!/bin/bash
sudo nmap -v -sn 192.168.23.129-254 -oG ping-sweep.txt
grep Up ping-sweep.txt | cut -d " " -f 2

(tmai@LAPTOP-EPF3I2KM) ~
$ chmod 777 task32.sh

(tmai@LAPTOP-EPF3I2KM) ~
$ ./task32.sh
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:43 +07
Initiating Ping Scan at 14:43
Scanning 126 hosts [4 ports/host]
Completed Ping Scan at 14:44, 19.11s elapsed (126 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:44
Completed Parallel DNS resolution of 1 host. at 14:44, 0.01s elapsed
Nmap scan report for 192.168.23.129 (192.168.23.129)
Host is up (0.0019s latency).
Nmap scan report for 192.168.23.130 [host down]
Nmap scan report for 192.168.23.131 [host down]
Nmap scan report for 192.168.23.132 [host down]
Nmap scan report for 192.168.23.133 [host down]
Nmap scan report for 192.168.23.134 [host down]
Nmap scan report for 192.168.23.135 [host down]
```

Hình 64. Nội dung và kết quả thực thi file task32.sh

- Kết quả scan:

```
Nmap done: 126 IP addresses (1 host up) scanned in 19.22 seconds
Raw packets sent: 1002 (38.056KB) | Rcvd: 92 (5.096KB)
192.168.23.129
```

Hình 65. Kết quả scan

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

→ Trả lời:

```
[tmai@LAPTOP-EPF3I2KM] ~
$ sudo nmap -sn 192.168.23.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 20:14 +07
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds
```

Hình 66. Khuyến cáo sử dụng -Pn khi sử dụng tùy chọn -sn nhưng không thành công

```
[tmai@LAPTOP-EPF3I2KM] ~
$ sudo nmap -Pn 192.168.23.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:08 +07
Nmap scan report for 192.168.23.129 (192.168.23.129)
Host is up (0.0057s 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

Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
```

Hình 67. Kết quả sử dụng nmap với tùy chọn -Pn

No.	Time	Source	Destination	Protocol	Length	Info
5	0.065041726	172.18.144.89	192.168.23.129	TCP	58	64056 - 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.065054792	172.18.144.89	192.168.23.129	TCP	58	64056 - 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.065059217	172.18.144.89	192.168.23.129	TCP	58	64056 - 5909 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.065063594	172.18.144.89	192.168.23.129	TCP	58	64056 - 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.065069027	172.18.144.89	192.168.23.129	TCP	58	64056 - 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	0.065073669	172.18.144.89	192.168.23.129	TCP	58	64056 - 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.065073389	172.18.144.89	192.168.23.129	TCP	58	64056 - 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.065076056	172.18.144.89	192.168.23.129	TCP	58	64056 - 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.065082529	172.18.144.89	192.168.23.129	TCP	58	64056 - 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.0650986642	172.18.144.89	192.168.23.129	TCP	58	64056 - 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.066789590	192.168.23.129	172.18.144.89	TCP	58	23 - 64056 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
16	0.066808410	192.168.23.129	172.18.144.89	TCP	58	111 - 64056 [TSN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
17	0.066783962	192.168.23.129	172.18.144.89	TCP	54	3389 - 64056 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	0.066784459	192.168.23.129	172.18.144.89	TCP	54	256 - 64056 [RST, ACK] Seq=3 Ack=1 Win=0 Len=0
19	0.066821370	192.168.23.129	172.18.144.89	TCP	58	80 - 64056 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
20	0.066821440	192.168.23.129	172.18.144.89	TCP	54	1720 - 64056 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	0.066830842	172.18.144.89	192.168.23.129	TCP	54	64056 - 80 [RST] Seq=0 Win=0 Len=0
22	0.066830828	172.18.144.89	192.168.23.129	TCP	54	64056 - 1 [RST] Seq=1 Win=0 Len=0
23	0.066830829	172.18.144.89	192.168.23.129	TCP	54	64056 - 22 [RST] Seq=1 Win=0 Len=0
24	0.066846938	192.168.23.129	172.18.144.89	TCP	54	1720 - 64056 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.066847809	192.168.23.129	172.18.144.89	TCP	54	113 - 64056 [RST, ACK] Seq=3 Ack=1 Win=0 Len=0
26	0.066847999	192.168.23.129	172.18.144.89	TCP	58	5998 - 64056 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
27	0.066913535	192.168.23.129	172.18.144.89	TCP	54	143 - 64056 [RST, ACK] Seq=1 Win=0 Len=0
28	0.066919311	172.18.144.89	192.168.23.129	TCP	54	64056 - 5909 [RST] Seq=1 Win=0 Len=0
29	0.067025212	172.18.144.89	192.168.23.129	TCP	58	64056 - 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	0.067030646	172.18.144.89	192.168.23.129	TCP	58	64056 - 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	0.067033645	172.18.144.89	192.168.23.129	TCP	58	64056 - 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	0.067036173	172.18.144.89	192.168.23.129	TCP	58	64056 - 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Hình 68. Kết quả bắt gói tin của wireshark

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

→ Trả lời:

- Máy ảo metasploitable:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:d3:ed:07
          inet addr:192.168.23.129 Bcast:192.168.23.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed3:ed07/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:8133 errors:34 dropped:37 overruns:0 frame:0
          TX packets:7326 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:554532 (541.5 KB) TX bytes:421284 (411.4 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:314 errors:0 dropped:0 overruns:0 frame:0
          TX packets:314 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:128645 (125.6 KB) TX bytes:128645 (125.6 KB)
```

Hình 69. Máy ảo metasploitable

- Sử dụng lệnh nmap -sV -sT -A 192.168.23.129

```
tmai@LAPTOP-EPF3I2KM:~$ 
$ nmap -sV -sT -A 192.168.23.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 13:21 +07
Nmap scan report for 192.168.23.129
Host is up (0.007s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.23.1
|   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:c1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
|_ssl-date: 2023-10-26T06:21:32+00:00; +5s from scanner time.
| sslv2:
|_ SSLv2 supported
| ciphers:
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| 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
```

```

|_Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
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 42630/tcp mountd
| 100005 1,2,3 43515/udp mountd
| 100021 1,3,4 38528/tcp nlockmgr
| 100021 1,3,4 58017/udp nlockmgr
| 100024 1 45152/udp status
| 100024 1 58128/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open tcpwrapped
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: 11
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, SwitchToSSLAfterHandshake, LongColumnFlag, SupportsTransactions, SupportsCompression, Speaks41ProtocolNew, Support41Auth
|   Status: Autocommit
|_ Salt: >PU;dgZj*.Ib5"EvF:0~

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-10-26T06:21:32+00:00; +5s 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
|_Not valid after: 2010-04-16T14:07:45
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
5600/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:04:53
|   source ident: nmap
|   source host: B825BBD7.FF91CB72.FFFA6D49.IP
|_ error: Closing Link: xiiyjvaiq[192.168.23.1] (Quit: xiiyjvaiq)
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-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m04s, deviation: 2h00m00s, median: 4s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:

| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2023-10-26T02:21:20-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.43 seconds

```

Hình 70, 71, 72, 74. Kết quả thực thi

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

→ Trả lời:

- Di chuyển đến thư mục /usr/share/nmap/scripts, kiểm tra các file NSE

```
tmai@LAPTOP-EPF312KM:~/usr/share/nmap/scripts]$ ls
$ ls
acarsd-info.nse          hostmap-crtsh.nse           ip-geolocation-map-bing.nse   rsync-brute.nse
address-info.nse          hostmap-robtex.nse          ip-geolocation-map-google.nse rsync-list-modules.nse
afp-brute.nse             http-adobe-coldfusion-apsa1301.nse ip-geolocation-map-kml.nse    rtsps-methods.nse
afp-ls.nse                http-affiliate-ld.nse        ip-geolocation-maxmind.nse   rtsps-url-brute.nse
afp-path-vuln.nse         http-apache-negotiation.nse ip-https-discover.nse       rusers.nse
afp-serverinfo.nse        http-apache-server-status.nse ipidseq.nse                  s7-info.nse
afp-showmount.nse         http-aspnets-debug.nse       ipmi-brute.nse              samba-vuln-cve-2012-1182.nse
ajp-auth.nse              http-auth-finder.nse       ipmi-cipher-zero.nse        script.db
ajp-brute.nse             http-auth.nse            ipmi-version.nse           servicetags.nse
ajp-headers.nse           http-avaya-ipoffice-users.nse ipv6-multicast-mld-list.nse shodan-api.nse
ajp-methods.nse           http-awstattotals-exec.nse  ipv6-node-info.nse         sip-brute.nse
ajp-request.nse           http-axis2-dir-traversal.nse  ipv6-ra-flood.nse          sip-call-spoof.nse
allseeingeye-info.nse     http-backup-finder.nse      irc-botnet-channels.nse    sip-enum-users.nse
ampq-info.nse             http-barracuda-dir-traversal.nse irc-brute.nse             sip-methods.nse
asn-query.nse              http-bigip-cookie.nse       irc-info.nse               skypev2-version.nse
```

Hình 74. Danh sách các file nse

- Sử dụng lệnh nmap -sV --script=banner 192.168.23.129

```
tmai@LAPTOP-EPF3I2KM:[/usr/share/nmap/scripts]
$ nmap -sv --script=banner 192.168.23.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 13:36 +07
Nmap scan report for 192.168.23.129
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (conn-refused)
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-Security
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     42630/tcp  mountd
|   100005  1,2,3     43515/udp mountd
|   100021  1,3,4     38528/tcp  nlockmgr
|   100021  1,3,4     58017/udp nlockmgr
|   100024  1          45152/udp status
|_  100024  1          58128/tcp  status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
|_banner: \x01Where are you?
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry

1524/tcp  open  bindshell   Metasploitable root shell
|_banner: root@metasploitable:/
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
| banner: >\x00\x00\x00\x00\x0A\x05.0.51a-3ubuntu5\x00\x18\x00\x00\x00\x00=y\x5X"\=\
|_...\x00,\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00...
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc        VNC (protocol 3.3)
|_banner: RFB 003.003
6000/tcp  open  x11        (access denied)
6667/tcp  open  irc        UnrealIRCd
| banner: :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostna
|_me...\\x0D\\x0A:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resol...
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.91 seconds
```

Hình 75, 76. Kết quả thực thi

- Sử dụng lệnh nmap -sV -script unusual-port 192.168.23.129

```
(tmai@LAPTOP-EPF3I2KM) [/usr/share/nmap/scripts]
$ nmap -sV --script unusual-port 192.168.23.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-26 13:43 +07
Nmap scan report for 192.168.23.129
Host is up (0.0033s 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-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     42630/tcp  mountd
|   100005  1,2,3     43515/udp mountd
|   100021  1,3,4     38528/tcp  nlockmgr
|   100021  1,3,4     58017/udp  nlockmgr
|   100024  1          45152/udp  status
|_ 100024  1          58128/tcp  status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
|_unusual-port: tcpwrapped unexpected on port tcp/514
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
|_unusual-port: java-rmi unexpected on port tcp/1099
1524/tcp  open  bindshell   Metasploitable root shell
|_unusual-port: bindshell unexpected on port tcp/1524
2049/tcp  open  nfs         2-4 (RPC #100003)
```

```
|_unusual-port: rpcbind unexpected on port tcp/2049
2121/tcp open  ftp          ProFTPD 1.3.1
|_unusual-port: ftp unexpected on port tcp/2121
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.05 seconds
```

Hình 77,78. Kết quả thực thi

---HẾT---