

2

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

THU THẬP THÔNG TIN

Information Gathering

Thực hành môn An toàn Mạng máy tính



Tháng 10/2023
Lưu hành nội bộ
<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

Mọi góp ý về tài liệu, vui lòng gửi về email inseclab@uit.edu.vn

A. TỔNG QUAN

1. Mục tiêu

- Thu thập thông tin của 1 cá nhân/tổ chức từ các nguồn trên Internet mà không cần tương tác với hệ thống thật.

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

3. Kiến thức nền tảng

Thu thập thông tin là giai đoạn đầu tiên trong quá trình kiểm thử xâm nhập. Đây là giai đoạn tốn nhiều thời gian và công sức nhất, nhưng cũng là yếu tố chính quyết định sự thành công hay thất bại của một chiến dịch. Càng có nhiều thông tin về đối tượng, chúng ta càng có thêm nhiều cơ hội khai thác vào đối tượng.

Mọi quy trình thu thập thông tin thường bao gồm 2 loại dữ liệu:

- Thu thập dữ liệu mạng: tên miền (public, private), các máy chủ, dãy IP public, private, bảng định tuyến, các dịch vụ TCP và UDP, chứng chỉ SSL, các port đang mở...
- Thu thập thông tin liên quan đến hệ điều hành: bao gồm thông tin user, hệ điều hành đang sử dụng, banner...
- Thu thập thông tin được chia làm 2 loại chính:
 - Thu thập thông tin thụ động (Passive Information Gathering)
 - Thu thập thông tin chủ động (Active Information Gathering)

4. Môi trường thực hành

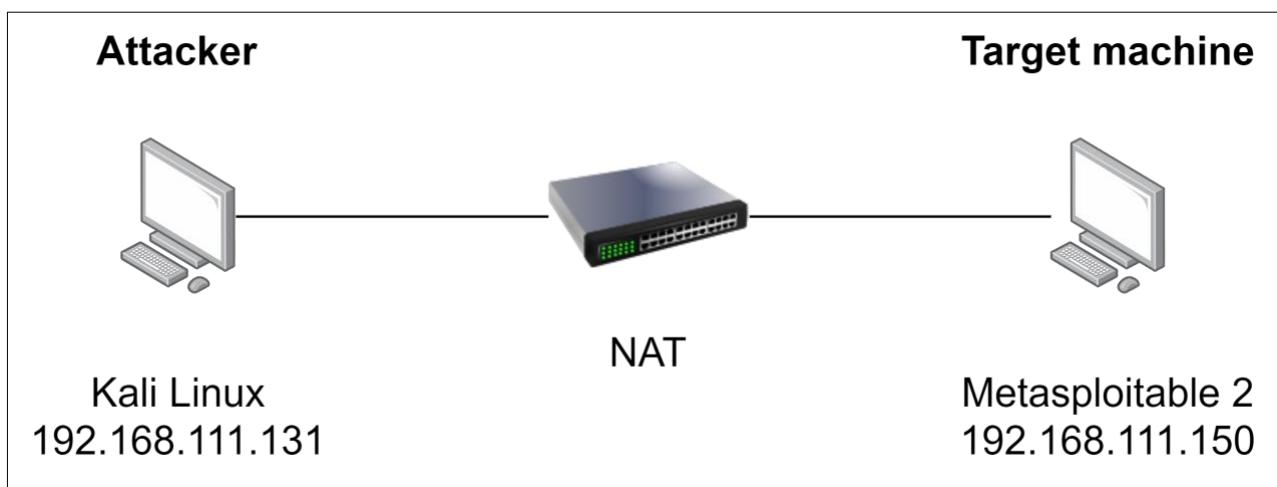
Sinh viên cần chuẩn bị trước máy tính với môi trường thực hành như sau:

Bài thực hành này sẽ sử dụng máy ảo Kali Linux đã được triển khai ở Lab 1.

Trong bài thực hành này, mục tiêu để thu thập thông tin là MegaCorp One.

Metasploitable 2 có địa chỉ IP 192.168.111.150 (VMNet 8 – NAT)

(<http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip>)



Hình 1. Mô hình mạng bài thực hành

B. THỰC HÀNH

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

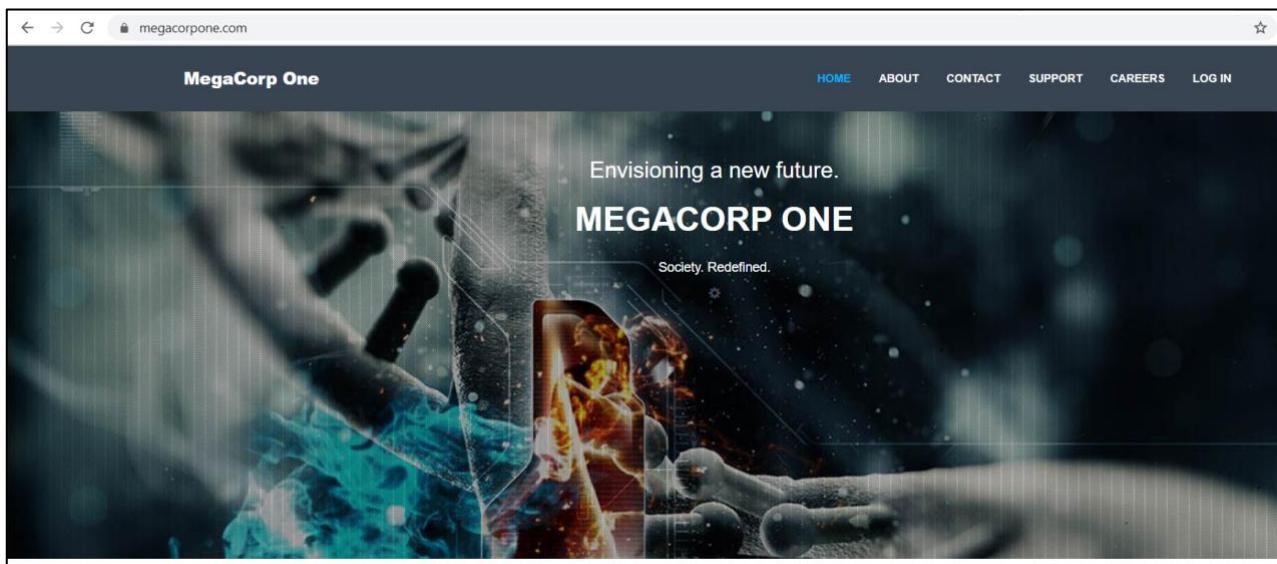
Thu thập thông tin thụ động (hay còn gọi là Open-source Intelligence hay OSINT) là quá trình thu thập các thông tin về đối tượng thông qua các phương tiện công cộng như Internet, tạp chí, báo, ... mà không có bất kỳ sự tương tác trực tiếp nào đến đối tượng đó. Có 2 cách thu thập thông tin thụ động:

- Cách 1: Chúng ta sẽ không bao giờ tương tác trực tiếp với đối tượng. Ví dụ, chúng ta có thể dựa vào kết quả từ bên thứ 3 để có được thông tin mà không truy cập vào bất kỳ hệ thống hoặc máy chủ nào của đối tượng. Việc sử dụng phương pháp này giúp ta giữ được tính bí mật về các hành động và ý định của mình, nhưng nhược điểm là có thể kết quả tìm kiếm sẽ bị giới hạn lại.
- Cách 2: Chúng ta có thể tương tác với đối tượng, nhưng chỉ như người dùng Internet bình thường. Ví dụ, nếu website của đối tượng cho phép chúng ta đăng ký tài khoản, chúng ta có thể thực hiện điều đó. Tuy nhiên, việc đánh giá website để tìm kiếm lỗ hổng sẽ không nằm trong giai đoạn này.

a) Do thám Website (Website Reconnaissance)

Nếu đối tượng có triển khai website, chúng ta có thể thu thập các thông tin cơ bản bằng cách truy cập vào website của đối tượng. Các tổ chức nhỏ có thể chỉ có duy nhất 1 website, trong khi các tổ chức lớn có thể có nhiều website. Vì vậy, việc thu thập thông tin các tổ chức lớn có thể mất khá nhiều thời gian, nhưng đổi lại thông tin có được về tổ chức đó sẽ nhiều hơn.

Thực hiện truy cập vào website của **MegaCorp One** tại (<https://www.megacorpone.com/>).



Hình 2. Trang web của tổ chức MegaCorp One

® Bài tập về nhà (yêu cầu làm)

1. Từ trang web của MegaCorp One, hãy mô tả một chút về lĩnh vực hoạt động của công ty?
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)?
3. Khi có được địa chỉ Email của các thành viên thuộc tổ chức, bạn có phát hiện ra điều gì?

b) Whois Enumeration

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

Chúng ta có thể thu thập các thông tin cơ bản về tên miền sử dụng công cụ **whois**.

```
root@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: 2020-06-16T17:05:41Z
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: 2020-08-20T07:51:25Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
```

Hình 3. Sử dụng whois trên tên miền megacorpone.com

Không phải tất cả dữ liệu đều có ích, nhưng chúng ta đã có thể lấy được một số thông tin có giá trị. Đầu tiên, kết quả whois cho ta biết được **Alan Grofield** là người đăng ký tên miền. Dựa vào trang giới thiệu công ty, ta biết được Alan là “IT and Security Director”.

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.	Quyền
Domain Name: megacorpone.com	Ngày sinh người được khai sinh
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN	TÌM KIEM
Registrar WHOIS Server: whois.gandi.net	TI
Registrar URL: http://www.gandi.net	
Updated Date: 2020-06-16T19:05:41Z	
Creation Date: 2013-01-22T23:01:00Z	
Registrar Registration Expiration 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	
Reseller:	
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited	
Domain Status:	
Registry Registrant ID:	
Registrant Name: Alan Grofield	
Registrant Organization: MegaCorpOne	
Registrant Street: 2 Old Mill St	
Registrant City: Rachel	
Registrant State/Province: Nevada	
Registrant Postal Code: 89001	
Registrant Country: US	
Registrant Phone: +1.9038836342	
Registrant Phone Ext:	
Registrant Fax:	
Registrant Fax Ext:	
Registrant Email: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net	NHẬP DỮ LIỆU TỪ FILE
Registry Admin ID:	Nhấn vào browse để chọn file (Dung lượng tối đa 3Mb và phải có định dạng .xml)
Admin Name: Alan Grofield	

Hình 4. Thông tin của người đăng ký tên miền

Ngoài ra, kết quả trả về của whois còn cho chúng ta biết được các name server của MegaCorp One. Name server là một trong những thành phần của DNS, và sẽ không được đề cập chi tiết trong bài thực hành này.

root@kali:~# whois megacorpone.com	Quyền
Domain Name: MEGACORPONE.COM	Ngày sinh người được khai sinh
Registry Domain ID: 1775445745_DOMAIN_COM-VRSN	TÌM KIEM
Registrar WHOIS Server: whois.gandi.net	TI
Registrar URL: http://www.gandi.net	
Updated Date: 2020-06-16T19:05:41Z	
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/	

Hình 5. Các name server đang quản lý tên miền megacorpone.com

® Bài tập về nhà (yêu cầu làm)

4. Sử dụng công cụ whois để xác định các name server của 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?
6. Thu thập thông tin về tên miền **uit.edu.vn** và hãy cho biết các thông tin như:
 - a. Ngày đăng ký tên miền
 - b. Ngày hết hạn tên miền
 - c. Chủ sở hữu tên miền
 - d. Các name server của tên miền

c) Google Hacking

Thuật ngữ “Google Hacking” trở nên phổ biến bởi Jonny Long vào năm 2001. Ông ấy đã chỉ ra cách sử dụng các search engine như Google có thể lấy được các thông tin, lỗ hổng quan trọng các website cấu hình sai.

Hãy thử một vài từ khóa cơ bản. Từ khóa **site** chỉ thực hiện tìm kiếm trên một tên miền nhất định.



site:megacorpone.com

About 25 results (0.19 seconds)

Try Google Search Console
www.google.com/webmasters/
Do you own **megacorpone.com**? Get indexing and ranking data from Google.

www.megacorpone.com ▾
MegaCorp One - Nanotechnology Is the Future ✓
We Create. Through years of experience, we have some of the most bleeding-edge technologies available to create opportunities that never seemed feasible.

www.megacorpone.com › assets ▾
Index of /assets - MegaCorp One ✓
Name · Last modified · Size · Description. [DIR], Parent Directory, -. [DIR], css/, 21-Aug-2016 11:21, -. [DIR], fonts/, 21-Aug-2016 11:21, -. [DIR], img/, 03-Oct-2017 ...

www.megacorpone.com ▾
400 Bad Request ✓
Bad Request. Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port.

www.megacorpone.com › about ▾
About Us - MegaCorp One ✓
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 ...

Hình 6. *Tìm kiếm với từ khóa site*

Từ khóa **filetype** (hoặc **ext**) để chỉ hiển thị các kết quả có phần mở rộng của tập tin theo chỉ định.



Google search results for "site:megacorpone.com filetype:html":

- [www.megacorpone.com › about](#)
About Us - MegaCorp One
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 ...
- [www.megacorpone.com › jobs](#)
Nanotechnology Is the Future - MegaCorp One
IT Positions. Citrix Administrator. Maintain, secure, and expand the MegaCorp One Citrix installation. Applicant must be well versed with remote work conditions ...
- [www.megacorpone.com › contact](#)
Contact Us - MegaCorp One
Name: Joe Sheer. Title: CEO Email: joe@megacorpone.com. Name: Mike Carlow. Title: VP Of Legal Email: mcarlow@megacorpone.com. Name: Alan Grofield.

Hình 7. Sử dụng từ khóa `filetype` để hiển thị các kết quả có phần mở rộng của tập tin theo chỉ định

Có thể thêm ký tự “-” để loại bỏ các kết quả tìm kiếm không mong muốn.

site:megacorpone.com -filetype:html

All Images News Shopping More Settings Tools

About 20 results (0.17 seconds)

[www.megacorpone.com › assets](#)

Index of /assets - MegaCorp One

Name · Last modified · Size · Description. [DIR], Parent Directory, -. [DIR], css/, 21-Aug-2016 11:21, -. [DIR], fonts/, 21-Aug-2016 11:21, -. [DIR], img/, 03-Oct-2017 ...

[www.megacorpone.com › assets › img](#)

400 Bad Request

Bad Request. Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port.

[www.megacorpone.com › assets › img](#)

Index of /assets/img - MegaCorp One

Name · Last modified · Size · Description. [DIR], Parent Directory, -. [IMG], agency.jpg, 21-Aug-2016 11:21, 166K. [IMG], browser.png, 21-Aug-2016 11:21, 211K.

[www.megacorpone.com › assets](#)

Index of /assets/js - MegaCorp One

Name · Last modified · Size · Description. [DIR], Parent Directory, -. [], bootstrap.min.js, 21-Aug-2016 11:21, 28K. [], custom.js, 21-Aug-2016 11:21, 368. [] ...

Hình 8. Sử dụng thêm ký tự “-” để loại bỏ các mục không mong muốn

Những ví dụ cơ bản trên chỉ là một số từ khóa thông dụng. Google Hacking Database (<https://www.exploit-db.com/google-hacking-database>) chứa nhiều từ khóa thường được sử dụng trong giai đoạn thu thập thông tin của đối tượng.

Date Added	Category	Author
2020-08-21	Files Containing Juicy Info	Anshul T
2020-08-21	Pages Containing Login Portals	Sibi Mathew George
2020-08-21	Various Online Devices	Alexandros Pappas
2020-08-20	Files Containing Juicy Info	Mayank Sharma
2020-08-20	Various Online Devices	Alexandros Pappas
2020-08-20	Various Online Devices	Alexandros Pappas
2020-08-20	Pages Containing Login Portals	Alexandros Pappas
2020-08-19	Pages Containing Login Portals	Adithya Chandra
2020-08-17	Various Online Devices	Jitendra Kumar Tripathi
2020-08-17	Pages Containing Login Portals	Edwyn Sanders
2020-08-17	Files Containing Passwords	Alexandros Pappas

Hình 9. Google Hacking Database (GHDB)

® Bài tập về nhà (yêu cầu làm)

7. Ai là Phó chủ tịch Pháp lý (Vice President of Legal) của MegaCorp One và địa chỉ email của họ là gì?
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?
9. Liệt kê một vài từ khóa thường gặp trên Google và cho ví dụ? (Yêu cầu: ít nhất 5 từ khóa)
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?

d) Netcraft

Netcraft là một công ty dịch vụ trên Internet có trụ sở tại Anh, cung cấp một cổng thông tin miễn phí thực hiện các chức năng thu thập thông tin khác nhau. Sử dụng các dịch vụ như Netcraft cung cấp được coi là một kỹ thuật thu thập thông tin thụ động vì chúng ta không bao giờ tương tác trực tiếp với đối tượng của mình.

Ví dụ: Netcraft cung cấp dịch vụ tìm kiếm thông tin DNS liên quan đến tên miền cần thu thập (<https://searchdns.netcraft.com/>).

The screenshot shows the Netcraft search interface. At the top, there is a search bar with the query "Hostnames matching *.megacorpone.com". Below the search bar, there is a search form with the following fields: "site contains" dropdown set to "site contains", a search term input field containing "*:megacorpone.com", and a "Search" button. Below the search form, there is a "Search tips" link. The main results section is titled "6 results" and displays a table with the following data:

Rank	Site	First seen	Netblock	OS	Site Report
1	www.megacorpone.com	March 2013	Amazon Data Services NoVa	Linux - Ubuntu	Report
2	www2.megacorpone.com	October 2015	Amazon Data Services NoVa	unknown	Report
3	siem.megacorpone.com	November 2016	Amazon Data Services NoVa	unknown	Report
4	intranet.megacorpone.com		Amazon Data Services NoVa	unknown	Report
5	support.megacorpone.com	May 2018	Amazon Data Services NoVa	unknown	Report
6	vpn.megacorpone.com	November 2016	Amazon Data Services NoVa	unknown	Report

Hình 10. Kết quả tìm kiếm các hostname chứa *.megacorpone.com

Ứng với mỗi máy chủ được tìm thấy, chúng ta có thể xem các thông tin bổ sung và lịch sử về máy chủ bằng cách sử dụng tính năng “Site Report”.

Background	Information	Value	
Site title	MegaCorp One - Nanotechnology Is the Future	Date first seen	March 2013
Site rank	104647	Netcraft Risk Rating	Not Present
Description	Not Present	Primary language	English

Network	Information	Value	Value
Site	http://www.megacorpone.com	Domain	megacorpone.com
Netblock Owner	Amazon Data Services NoVa	Nameserver	ns1.megacorpone.com
Hosting company	Amazon - US East (Northern Virginia) datacenter	Domain registrar	gandi.net
Hosting country	US	Nameserver organisation	whois.gandi.net
IPv4 address	3.220.87.155 (VirusTotal)	Organisation	MegaCorpOne, Rachel, 89001, United States
IPv4 autonomous systems	AS14618	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	ec2-3-220-87-155.compute-1.amazonaws.com		

Hình 11. Site Report đối với máy chủ www.megacorpone.com

® Bài tập về nhà (Cộng điểm)

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

e) Recon-ng

Recon-ng là một nền tảng theo module cho mục đích thu thập thông tin dựa trên web. Recon-ng hiển thị kết quả trên terminal hoặc CSDL. Điểm mạnh của recon-ng là có thể đưa kết quả từ module này làm đầu vào cho module khác, cho phép chúng ta nhanh chóng mở rộng phạm vi thu thập thông tin của mình. Để sử dụng, thực hiện lệnh **recon-ng**.

Hình 12. *Khởi động recon-ng*

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

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

+-----+-----+-----+-----+-----+
|          Path          | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/companies-multi/github_miner | 1.1    | not installed | 2020-05-15 |   | * |
| recon/profiles-contacts/github_users | 1.0    | not installed | 2019-06-24 |   | * |
| recon/profiles-profiles/profiler | 1.0    | not installed | 2019-06-24 |   |   |
| recon/profiles-repositories/github_repos | 1.1    | not installed | 2020-05-15 |   | * |
| recon/repositories-profiles/github_commits | 1.0    | not installed | 2019-06-24 |   | * |
| recon/repositories-vulnerabilities/github_dorks | 1.0    | not installed | 2019-06-24 |   | * |
+-----+-----+-----+-----+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.
```

Hình 13. Tìm kiếm các module chưa từ khóa github

Dựa vào Hình 13, lưu ý cột “K”, chúng ta thấy có một số module được đánh dấu *. Các module này yêu cầu cung cấp thông tin đăng nhập hoặc API key cho các nhà cung cấp bên thứ 3. Một vài key sẽ được miễn phí nếu đăng ký tài khoản, trong khi sẽ có một vài key yêu cầu trả phí.

Sử dụng lệnh **marketplace info** để biết thông tin của module.

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

Hình 14. Thông tin về module có yêu cầu key

```
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web
+---+
| path      | recon/domains-hosts/google_site_web
| name      | Google Hostname Enumerator
| author    | Tim Tomes (@lanmaster53)
| version   | 1.0
| last_updated | 2019-06-24
| description | Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.
| required_keys | []
| dependencies | []
| files     | []
| status     | not installed
+---+
```

Hình 15. Thông tin về module không cần key

Sử dụng lệnh **marketplace install** để thực hiện cài đặt module.

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

Hình 16. Cài đặt module

Sau khi cài đặt module, sử dụng lệnh **modules load** để sử dụng module đó. Sau đó dùng lệnh **info** để hiển thị thông tin chi tiết về module và các tham số yêu cầu.

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

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

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

Options:
    Name      Current Value  Required  Description
    -----  -----  -----  -----
    SOURCE    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

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

Hình 17. Sử dụng module `recon/domains-hosts/netcraft`

Dựa vào kết quả Hình 17, module này yêu cầu tham số đầu vào là **source**, là đối tượng mà chúng ta cần thu thập thông tin. Trong trường hợp này, sử dụng lệnh **options set SOURCE megacorpone.com** để thiết lập tên miền của mục tiêu.

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

Hình 18. Thiết lập mục tiêu cần thu thập thông tin

Chạy lệnh **run** để chạy module.

```
[recon-ng][default][netcraft] > run
-----
[MEGACORPONE.COM]
-----
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=megacorpone.com
[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: vpn.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: siem.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: www2.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: intranet.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: support.megacorpone.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
SUMMARY
-----
[*] 6 total (6 new) hosts found.
[recon-ng][default][netcraft] >
```

Hình 19. Chạy module

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

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

+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+-----+
| 1 | www.megacorpone.com | | | | | | netcraft |
| 2 | vpn.megacorpone.com | | | | | | netcraft |
| 3 | siem.megacorpone.com | | | | | | netcraft |
| 4 | www2.megacorpone.com | | | | | | netcraft |
| 5 | intranet.megacorpone.com | | | | | | netcraft |
| 6 | support.megacorpone.com | | | | | | netcraft |
+-----+
[*] 6 rows returned
```

Hình 20. Xem lịch sử các host

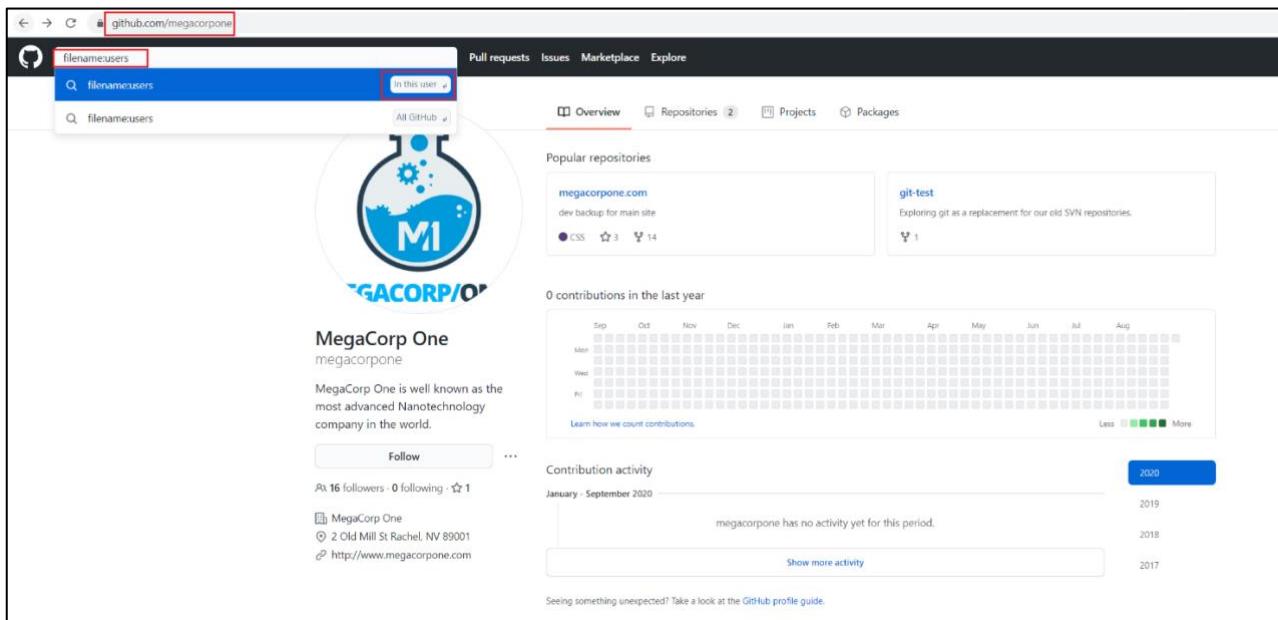
Bài tập về nhà (Yêu cầu làm)

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

f) Open-Source Code

Một trong những nơi để thu thập thông tin là ở những nơi lưu trữ mã nguồn mở, tập trung như GitHub, GitLab, SourceForge.

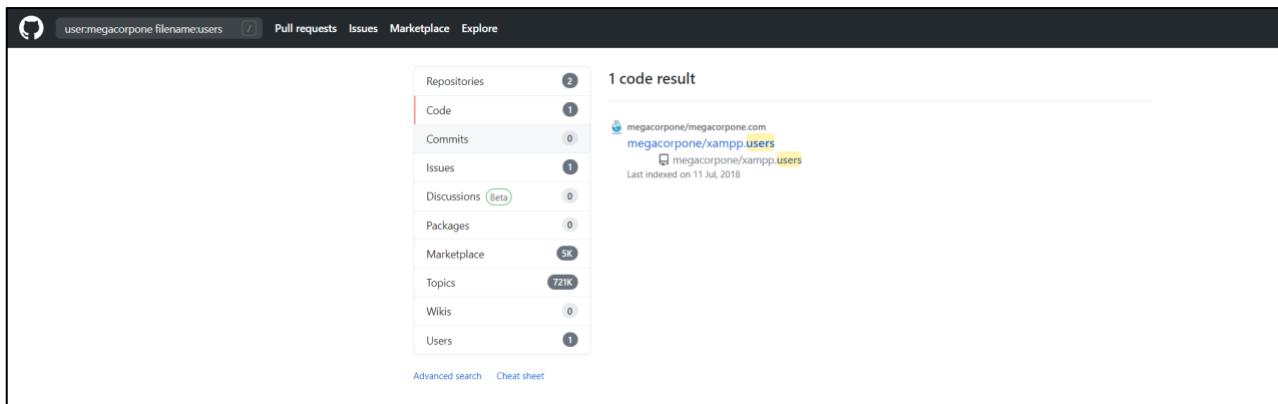
Truy cập vào GitHub của MegaCorp One (<https://github.com/megacorpone>), sử dụng từ khóa **file:users** để tìm kiếm các tập tin có chứa từ khóa “users”.



Hình 21. Tìm kiếm tập tin trong GitHub

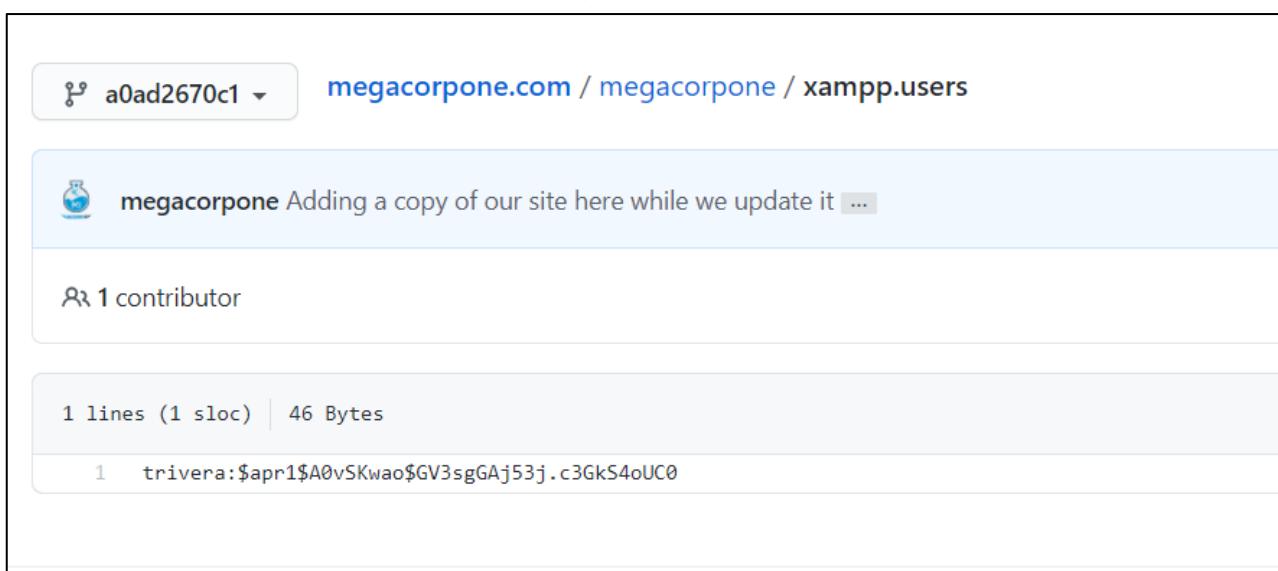
Truy cập vào GitHub của MegaCorp One (<https://github.com/megacorpone>), sử dụng từ khóa **file:users** để tìm kiếm các tập tin có chứa từ “users”.

Kết quả tìm kiếm chỉ trả về một tập tin duy nhất – **xampp.users**. Tuy nhiên, lưu ý XAMPP là môi trường phát triển ứng dụng web, vì vậy có thể xem đây là 1 phát hiện khá có ích.



Hình 22. Kết quả trả về sau khi tìm kiếm trên GitHub

Kiểm tra nội dung của tập tin này. Tập tin này chứa tên đăng nhập và mật khẩu (dưới dạng mã hash), sẽ rất có ích trong các giai đoạn sau.



Hình 23. Nội dung tập tin xampp.users chứa username và password (dạng hash)

Tuy nhiên, hướng tiếp cận này sẽ hoạt động tốt nhất đối với các repository nhỏ. Đối với các repo lớn hơn, chúng ta có thể sử dụng thêm các công cụ để giúp tự động tìm kiếm như Gitrob (<https://github.com/michenriksen/gitrob>), Gitleaks (<https://github.com/zricethezav/gitleaks>).

® Bài tập về nhà (Cộng điểm)

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

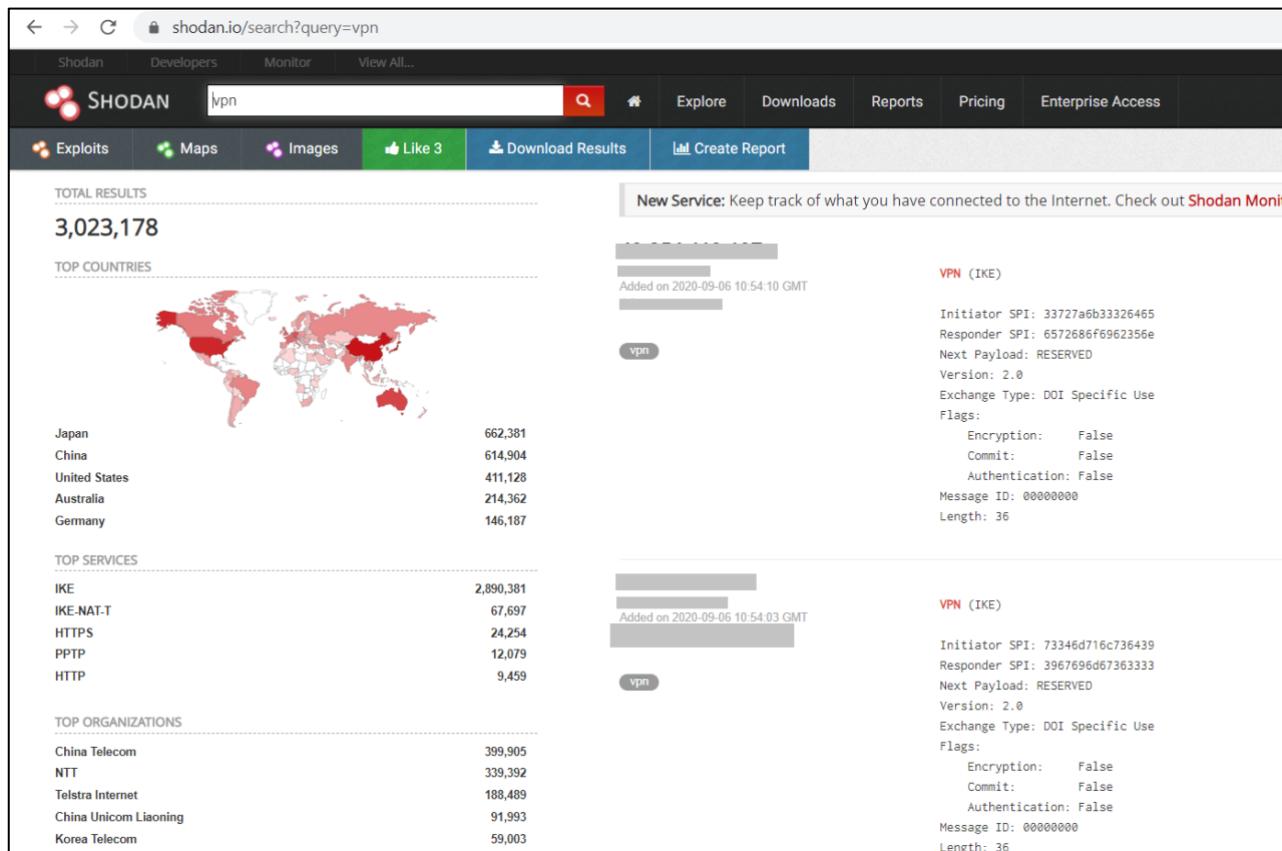
g) Shodan

Shodan (<https://www.shodan.io/>) là một search engine thu thập thông tin bất kỳ thiết bị nào được kết nối Internet, bao gồm các máy chủ web, các router, thiết bị IoT, ...

Nói một cách khác, Google và các search engine khác chỉ thực hiện việc tìm kiếm nội dung trên các máy chủ web, trong khi Shodan tìm kiếm các thiết bị được kết nối Internet, tương tác với chúng, và hiển thị thông tin về chúng.

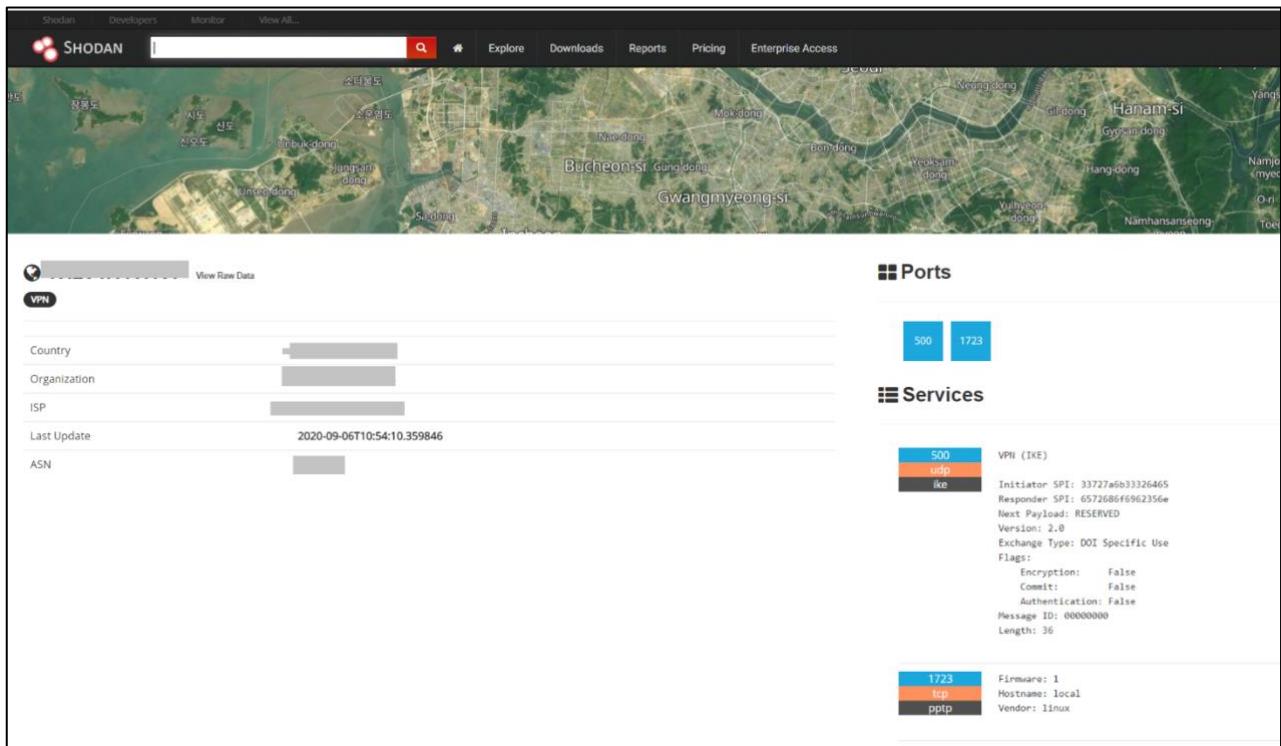
Trước khi sử dụng Shodan, chúng ta phải thực hiện đăng ký tài khoản.

Ví dụ, để tìm kiếm các máy chủ đang chạy dịch vụ VPN, nhập lệnh **vpn** trên ô tìm kiếm.



Hình 24. Tìm kiếm các VPN Server trên thế giới

Từ kết quả trả về, chúng ta có thể nhìn thấy các port, dịch vụ, công nghệ được sử dụng bởi server. Shodan cũng sẽ cho ta biết kết quả nếu các dịch vụ, công nghệ được phát hiện trên máy chủ có tồn tại lỗ hổng hay không.



Hình 25. Thông tin chi tiết của 1 máy chủ trên Shodan

⑧ Bài tập về nhà (Cộng điểm)

15. Thực hiện tìm kiếm các lệnh khác trên Shodan mà có thể tiết lộ thêm nhiều thông tin thú vị về một đối tượng bất kỳ.
16. So sánh kết quả tìm kiếm trên Shodan so với các search engine khác như Google, Bing...

h) theHarvester

theHarvester là công cụ giúp thu thập địa chỉ email, địa chỉ IP, URL từ các nguồn khác nhau. Ví dụ, sử dụng theHarvester với tùy chọn **-d** để chỉ định tên miền của mục tiêu và **-b** để chỉ định nguồn tìm kiếm.

```
root@kali:~# theHarvester -d megacorpone.com -b goo
```

Hình 26. Sử dụng công cụ theHarvester

Trong danh sách các địa chỉ email được trả về, “first@megacorpone.com” được xem như là địa chỉ email mới, chưa được phát hiện bằng các công cụ khác. Ngoài ra, chúng ta còn phát hiện thêm được các subdomain khác.

Điều này chứng tỏ, không phải công cụ nào cũng cho ta kết quả đầy đủ. Việc kết hợp nhiều công cụ sẽ giúp ta có được nhiều thông tin về đối tượng hơn.

[®] Bài tập về nhà (Cộng điểm)

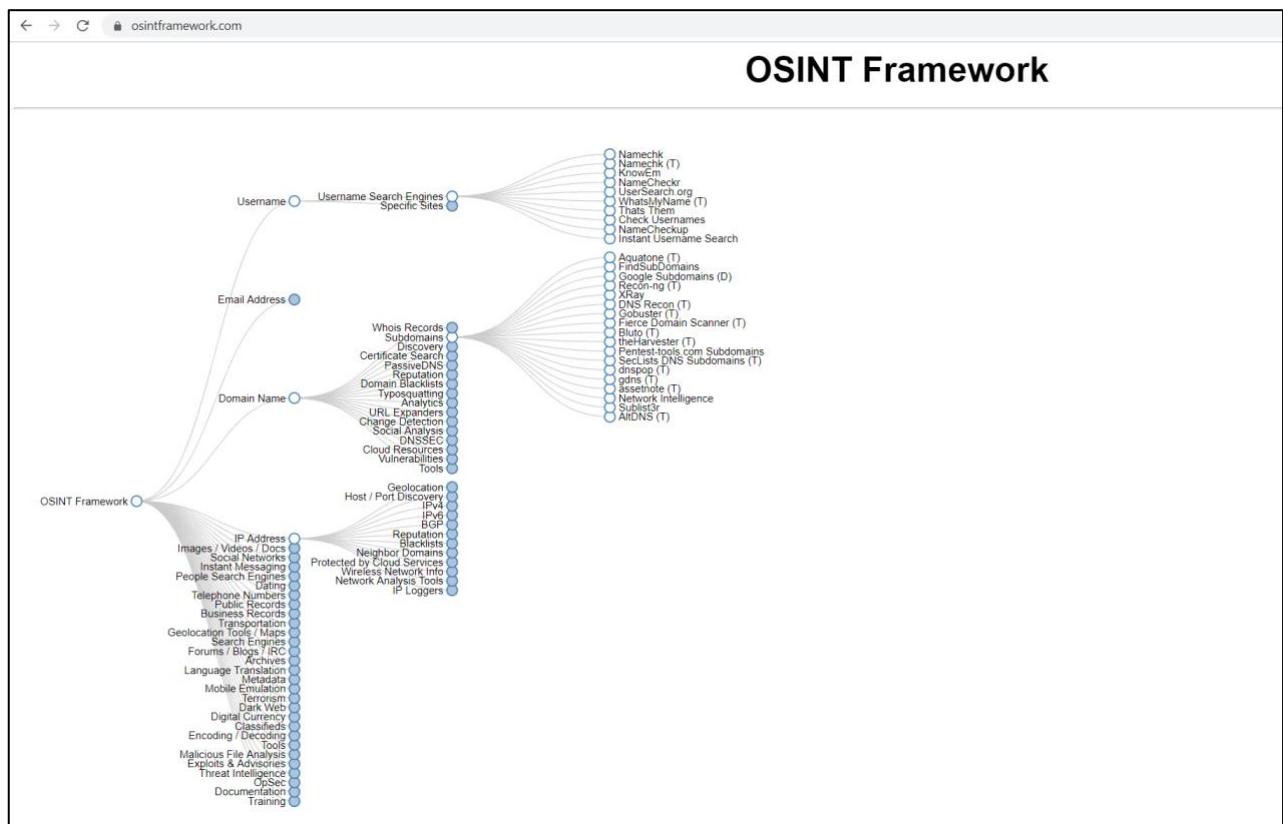
17. Sử dụng công cụ theHarvester để lấy tìm kiếm các địa chỉ email của UIT

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

i) Information Gathering Frameworks

OSINT Framework

OSINT Framework (<https://osintframework.com/>) là một nơi lưu trữ thông các công cụ và website phục vụ cho giai đoạn thu thập thông tin. OSINT Framework không phải là một checklist, nhưng việc xem xét các danh mục cũng như các công cụ có sẵn có thể giúp ta thu thập được nhiều thông tin về đối tượng càng tốt.



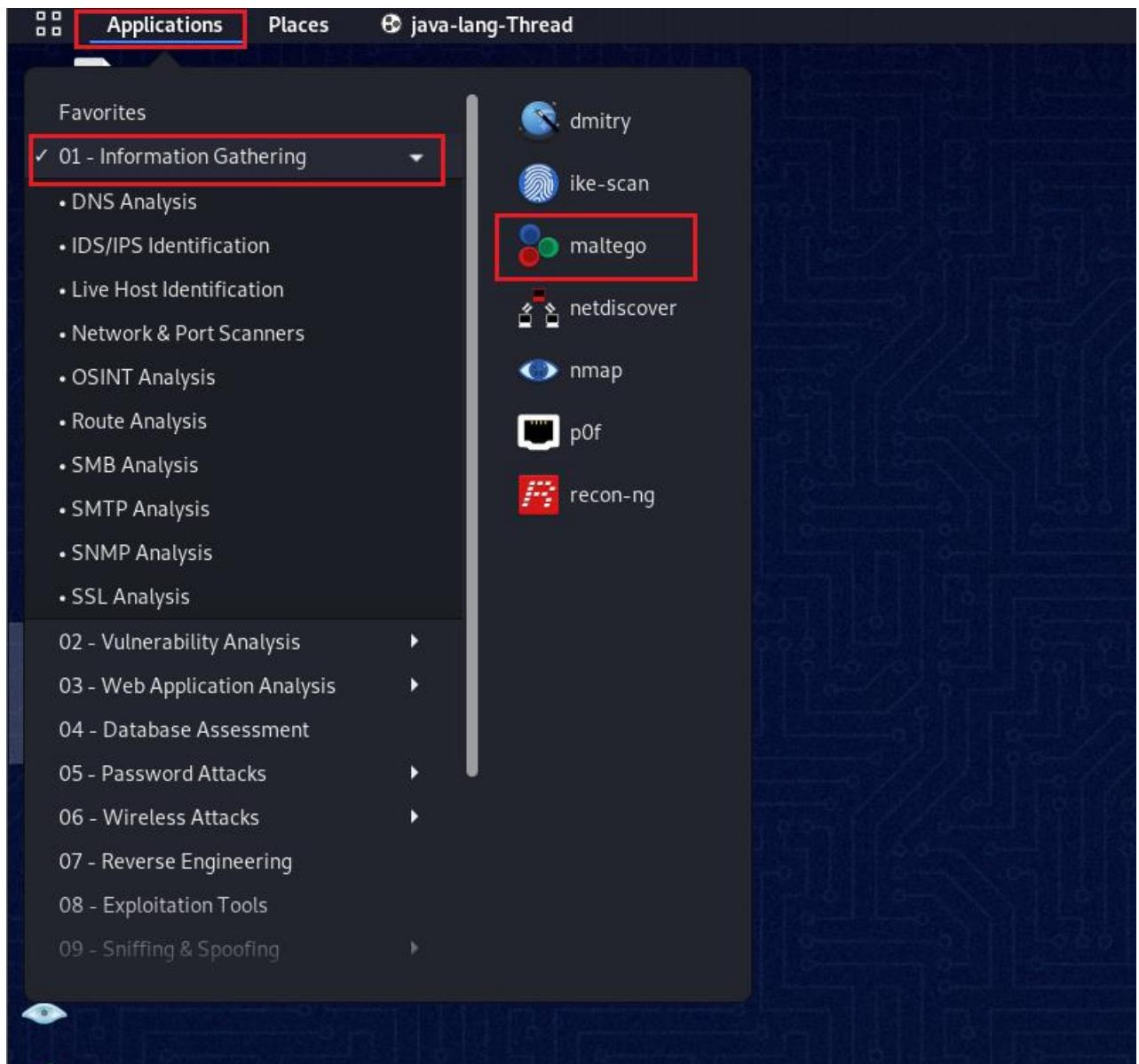
Hình 27. OSINT Framework

Maltego

Maltego là một dự án mã nguồn mở và được phát triển bởi Paterva. Công cụ này có thể tìm mối quan hệ giữa các thông tin thu thập được và cung cấp dữ liệu cấu trúc về các thông tin đó, một đặc tính làm cho Maltego khác biệt so với các công cụ khác.

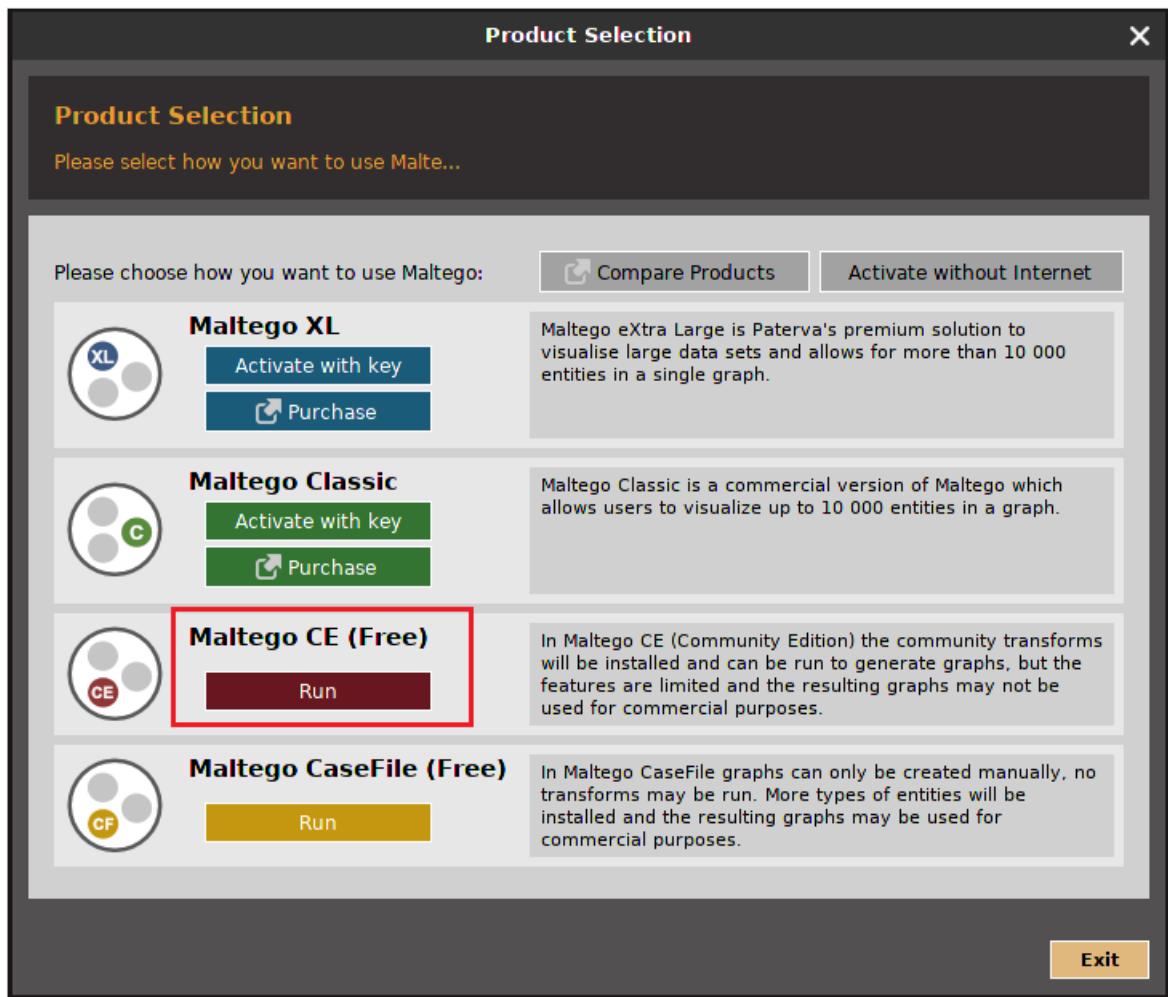
Maltego cung cấp các tùy chọn tìm kiếm mạnh mẽ cho người dùng và hiển thị kết quả trực quan và thông minh hơn các công cụ khác.

Maltego được cài đặt sẵn trong Kali Linux nhưng nó không phải là phiên bản đầy đủ. Có thể nói nó là phiên bản dùng thử hoặc phiên bản cộng đồng. Nó có một phiên bản trả phí và nó cung cấp nhiều tùy chọn tìm kiếm hơn và cho kết quả tốt hơn nhiều.



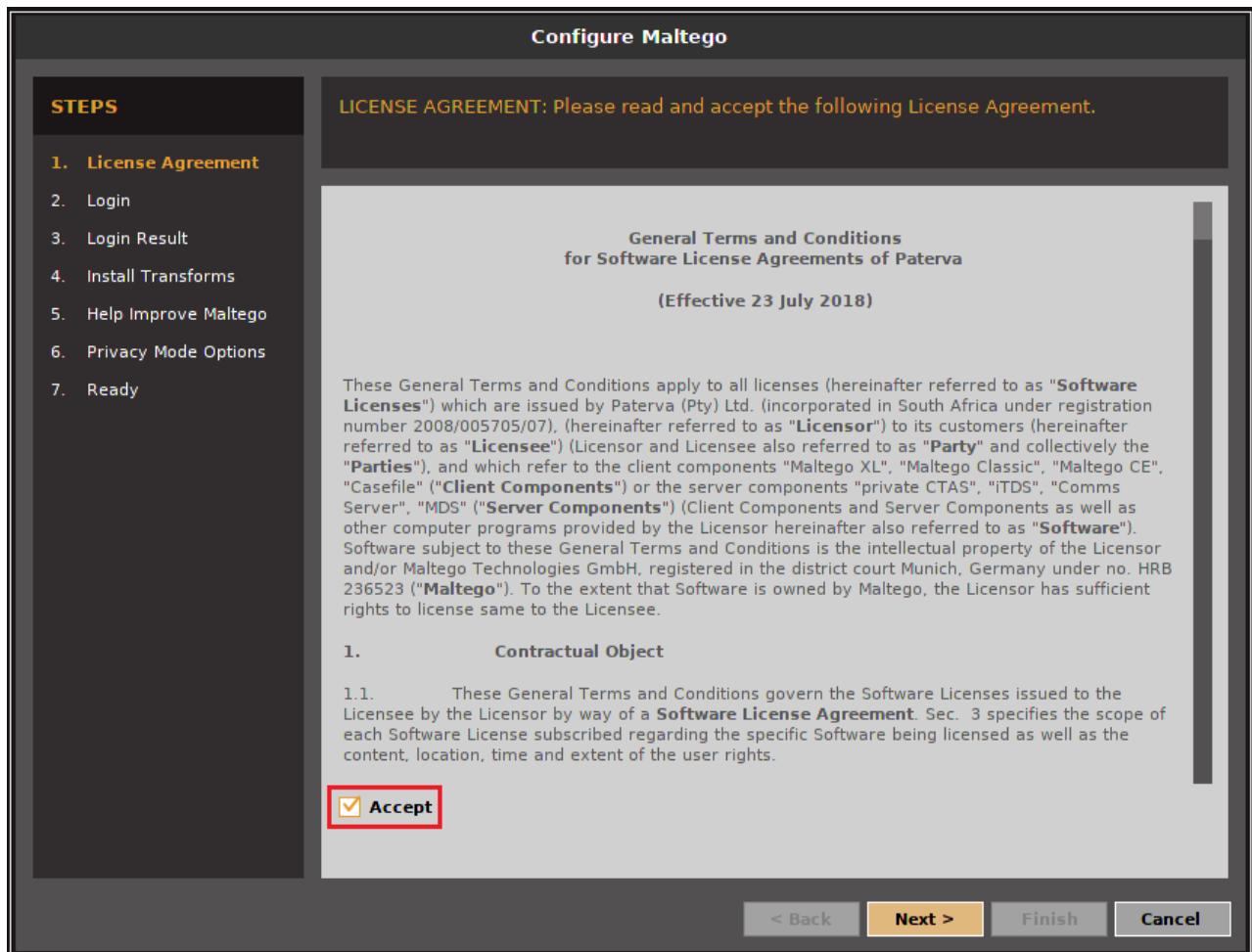
Hình 28. Khởi động Maltego trên Kali Linux

Chọn **Maltego CE (Free)** để khởi động Maltego ở phiên bản Community.



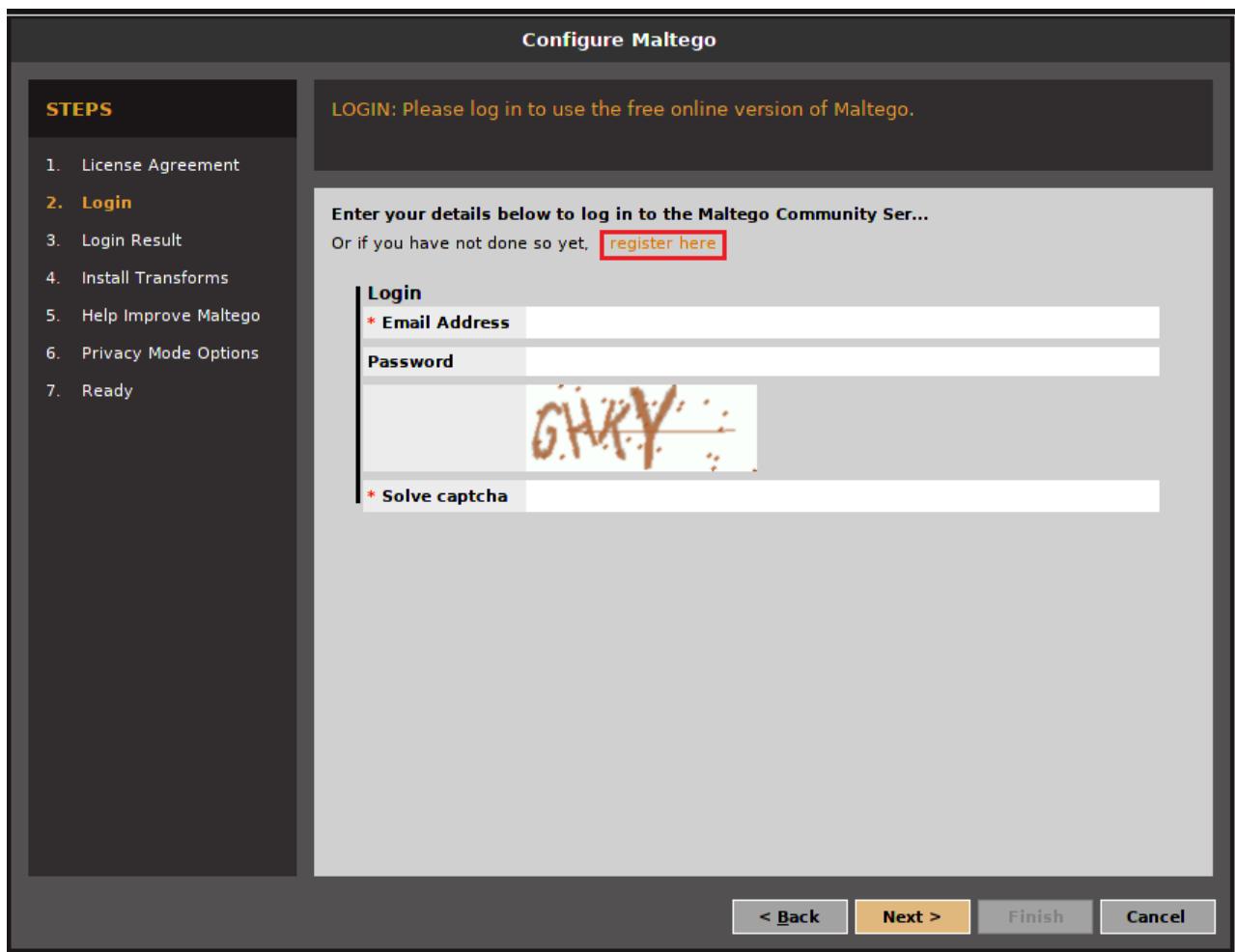
Hình 29. Sử dụng phiên bản Maltego CE

Chọn **Accept** để chấp nhận điều khoản sử dụng.



Hình 30. Chấp nhận điều khoản sử dụng

Thực hiện đăng ký tài khoản (nếu chưa có).



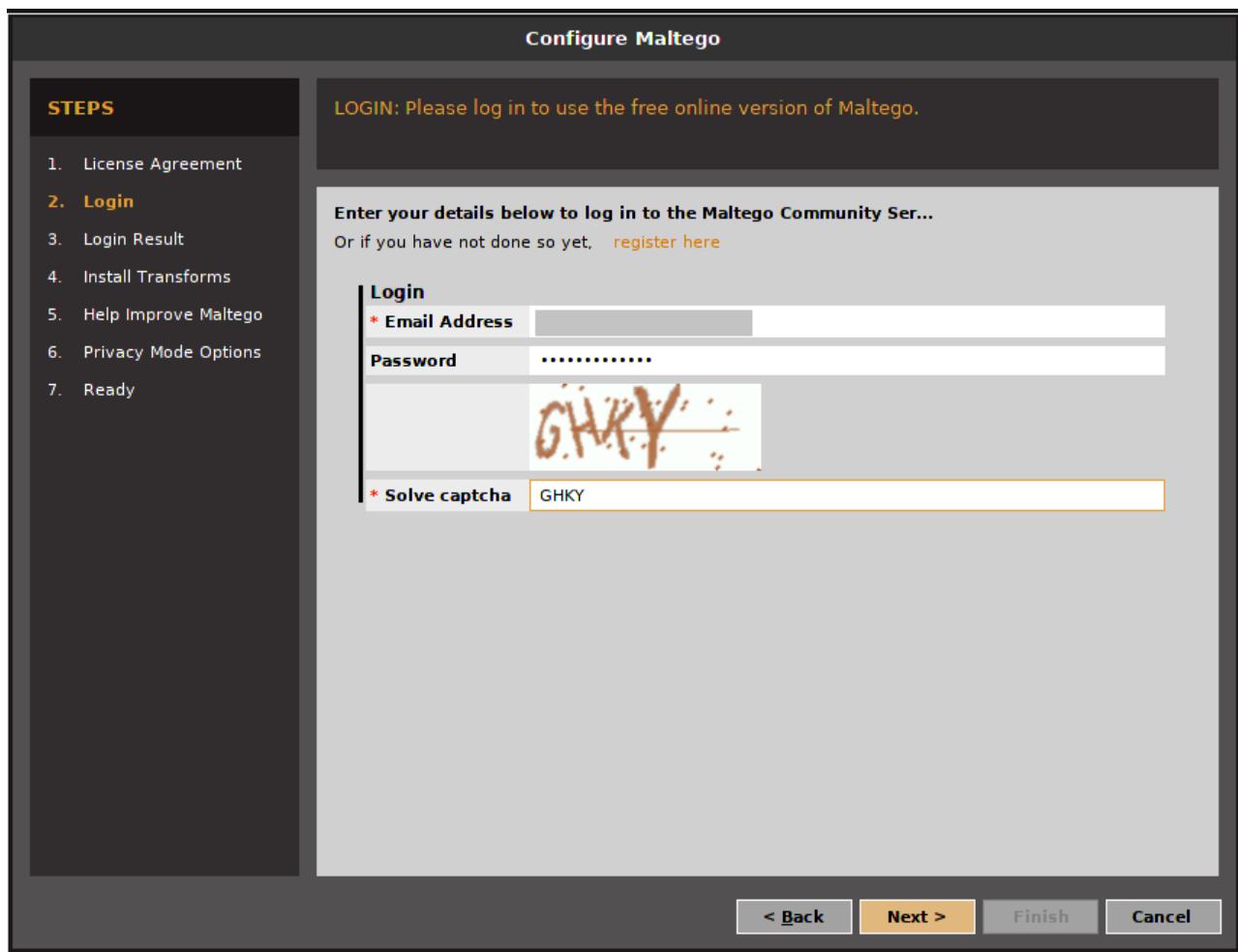
Hình 31. Thực hiện đăng ký tài khoản

Điền các thông tin theo yêu cầu để tiến hành tạo tài khoản mới.

The screenshot shows the 'Register a Maltego CE Account' page. The URL is https://www.maltego.com/ce-registration/. The page has fields for FIRST NAME, LAST NAME, EMAIL, and two PASSWORD fields. Below the form is a message about existing accounts and links for password reset. A CAPTCHA is present, and at the bottom is a yellow 'REGISTER' button.

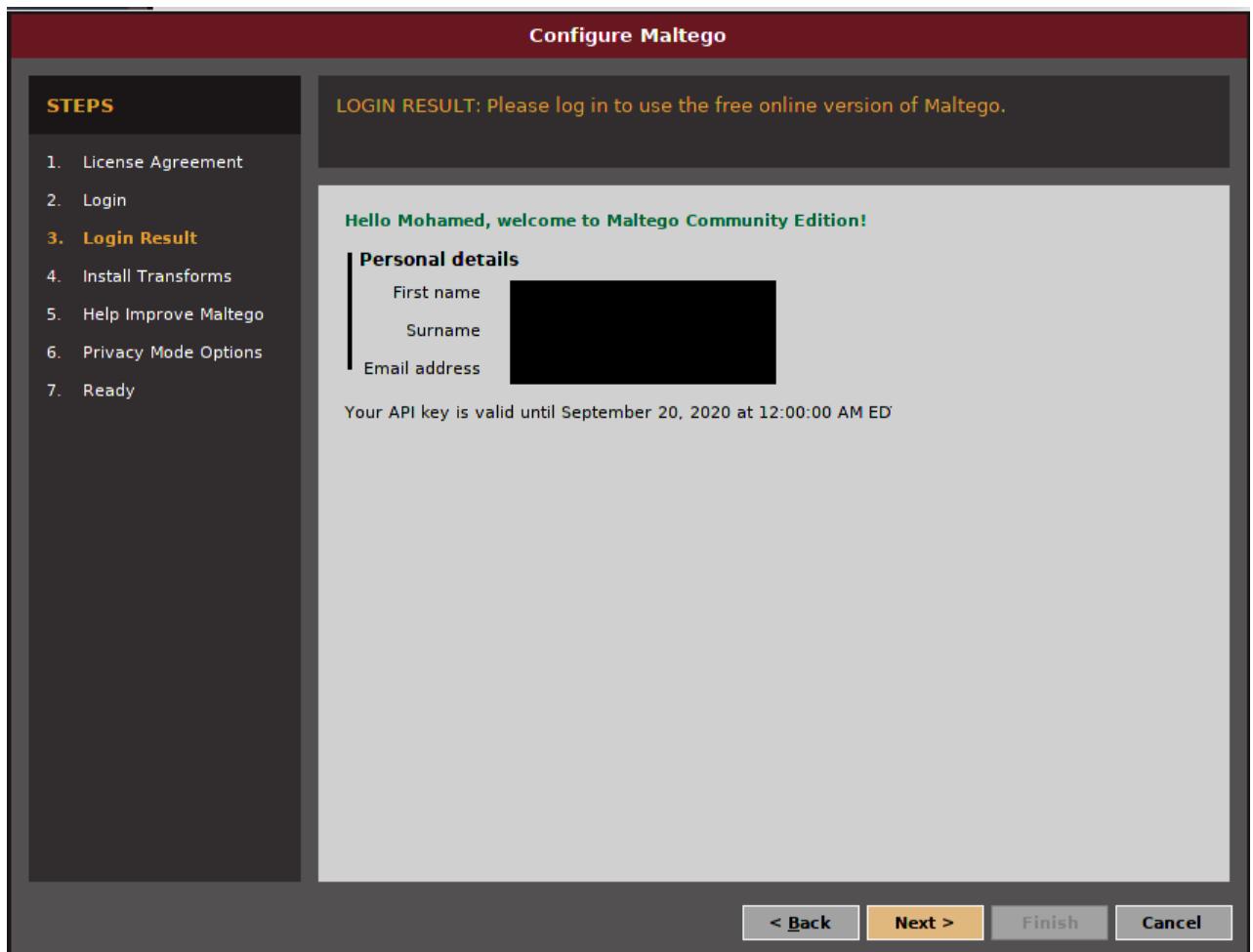
Hình 32. Điền vào form đăng ký tài khoản

Sau khi đăng ký và kích hoạt tài khoản qua Email, thực hiện nhập thông tin ở Hình 32.



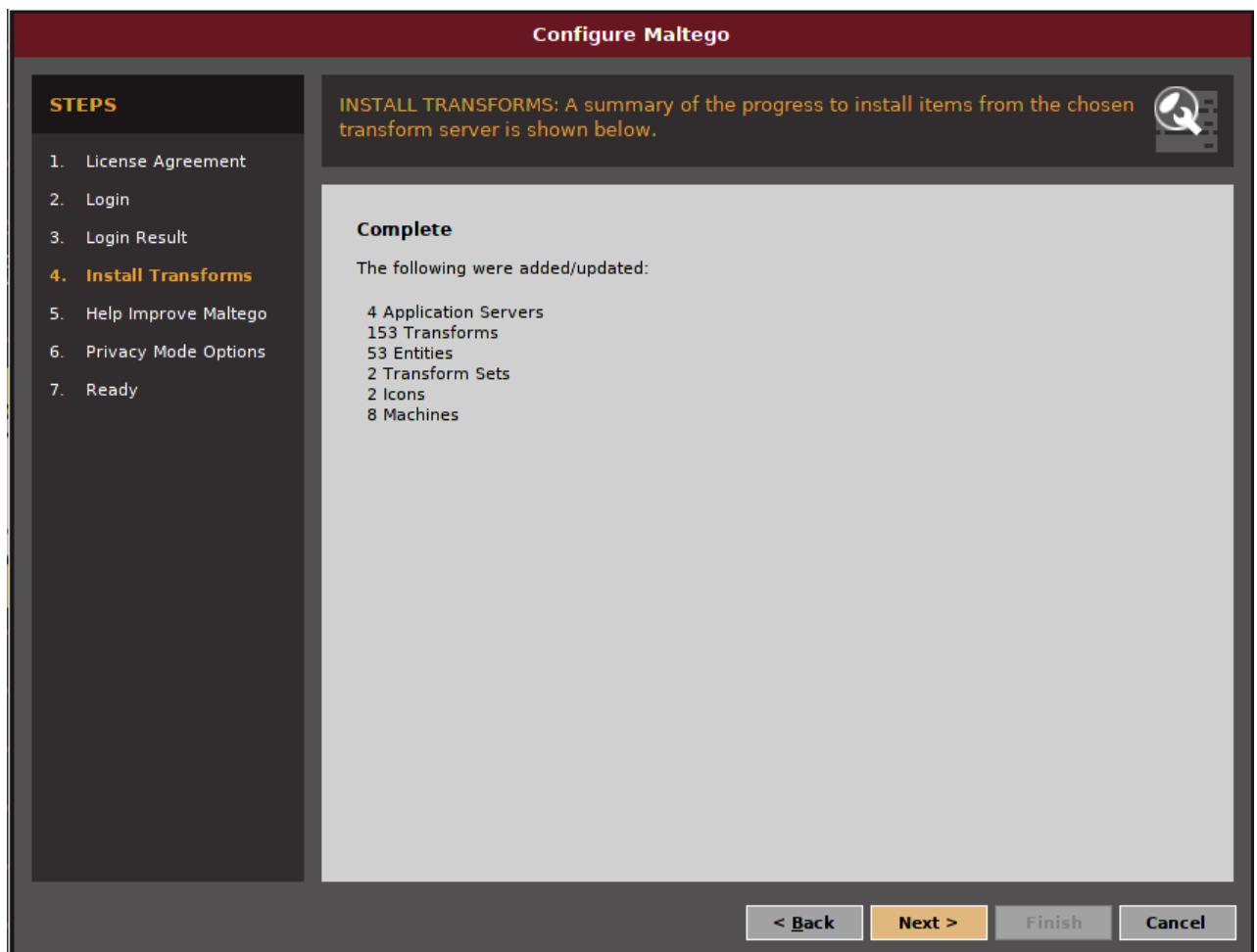
Hình 33. Nhập thông tin tài khoản vừa đăng ký

Hộp thoại kiểm tra lại thông tin, chọn Next



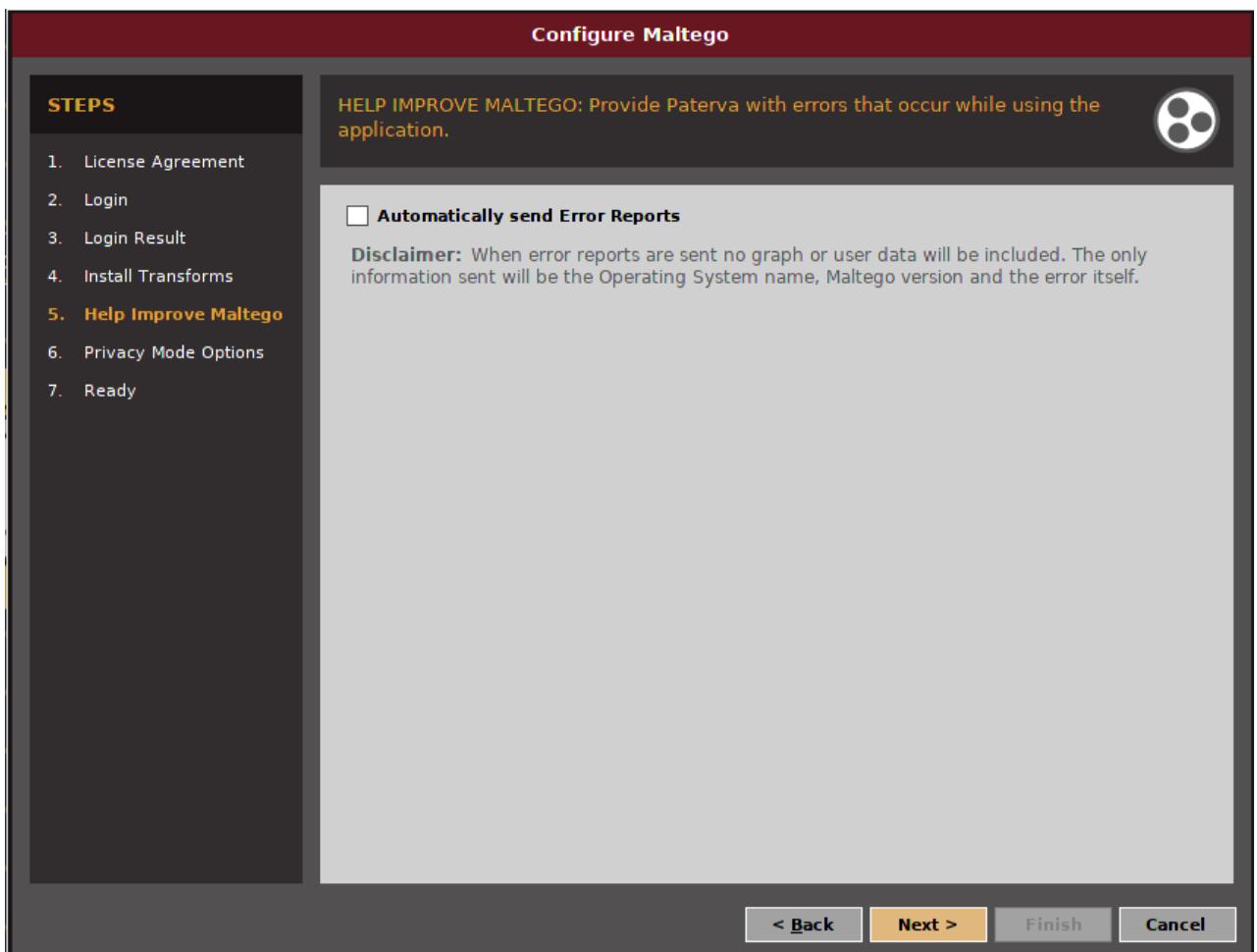
Hình 34. Kiểm tra lại thông tin đăng nhập

Hộp thoại thông tin cài đặt, chọn Next.



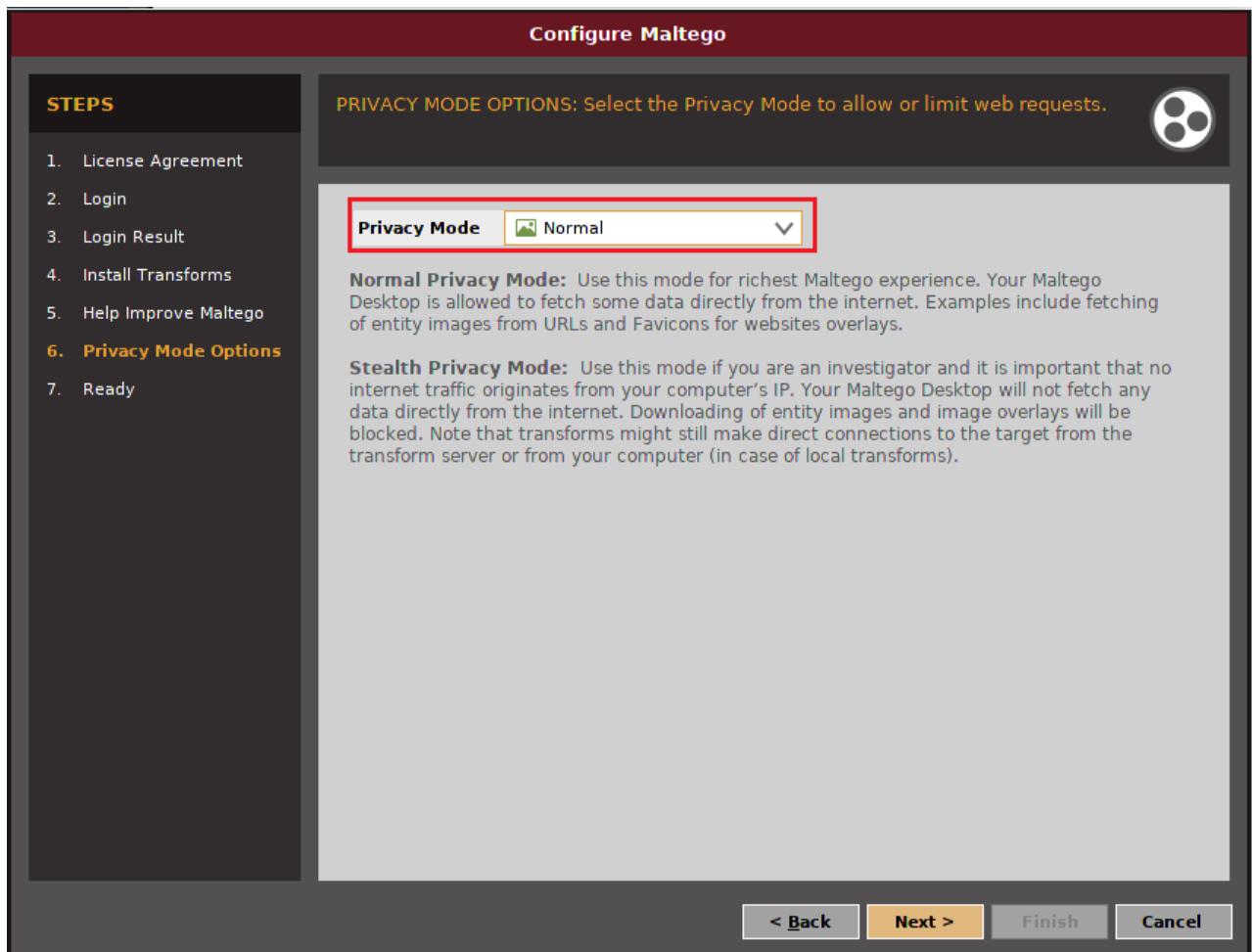
Hình 35. *Hộp thoại thông tin cài đặt*

Giữ nguyên mặc định, chọn Next



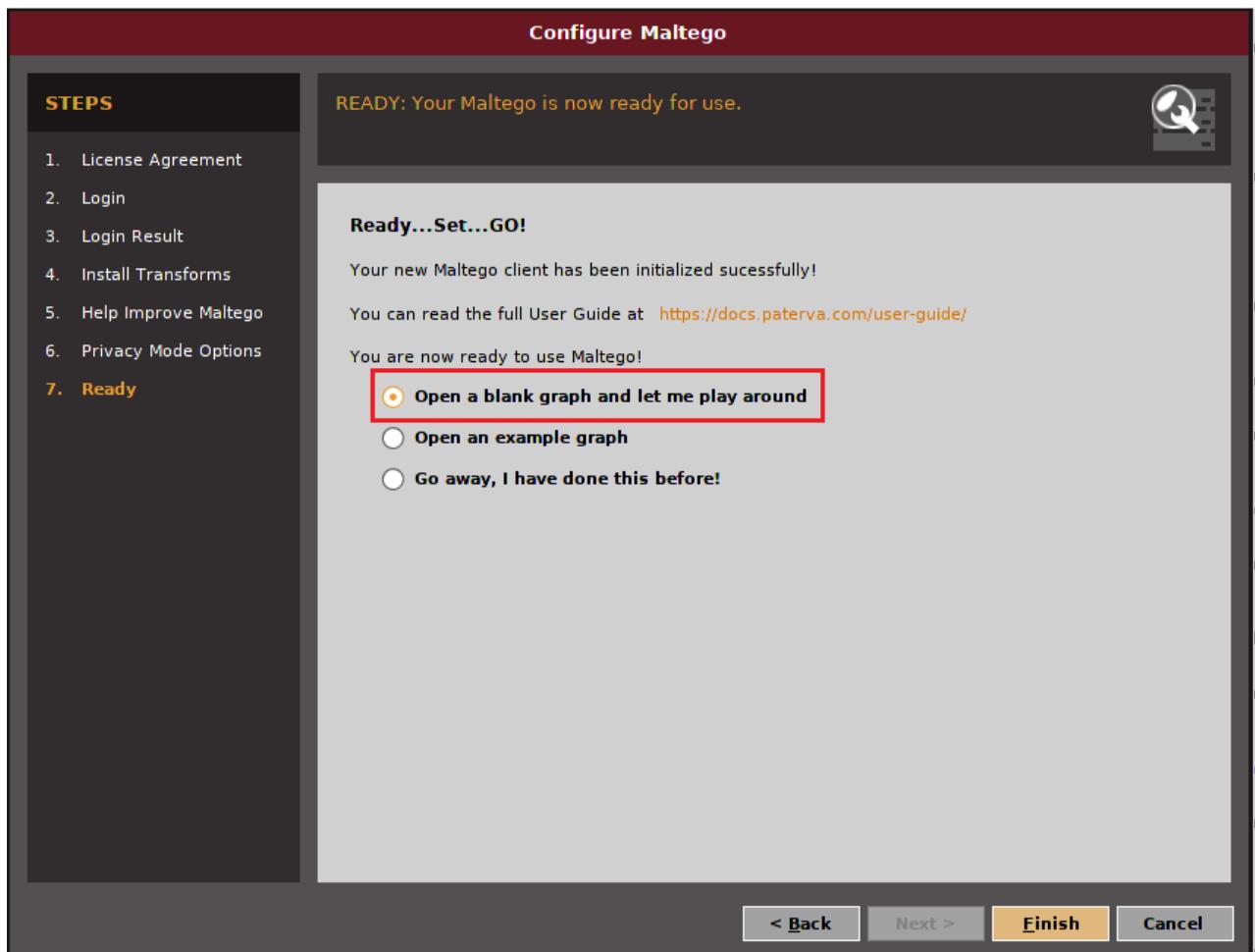
Hình 36. *Hộp thoại giúp cải thiện Maltego được tốt hơn*

Mục Privacy Mode, chọn Normal



Hình 37. Chọn chế độ Normal trong Privacy Mode

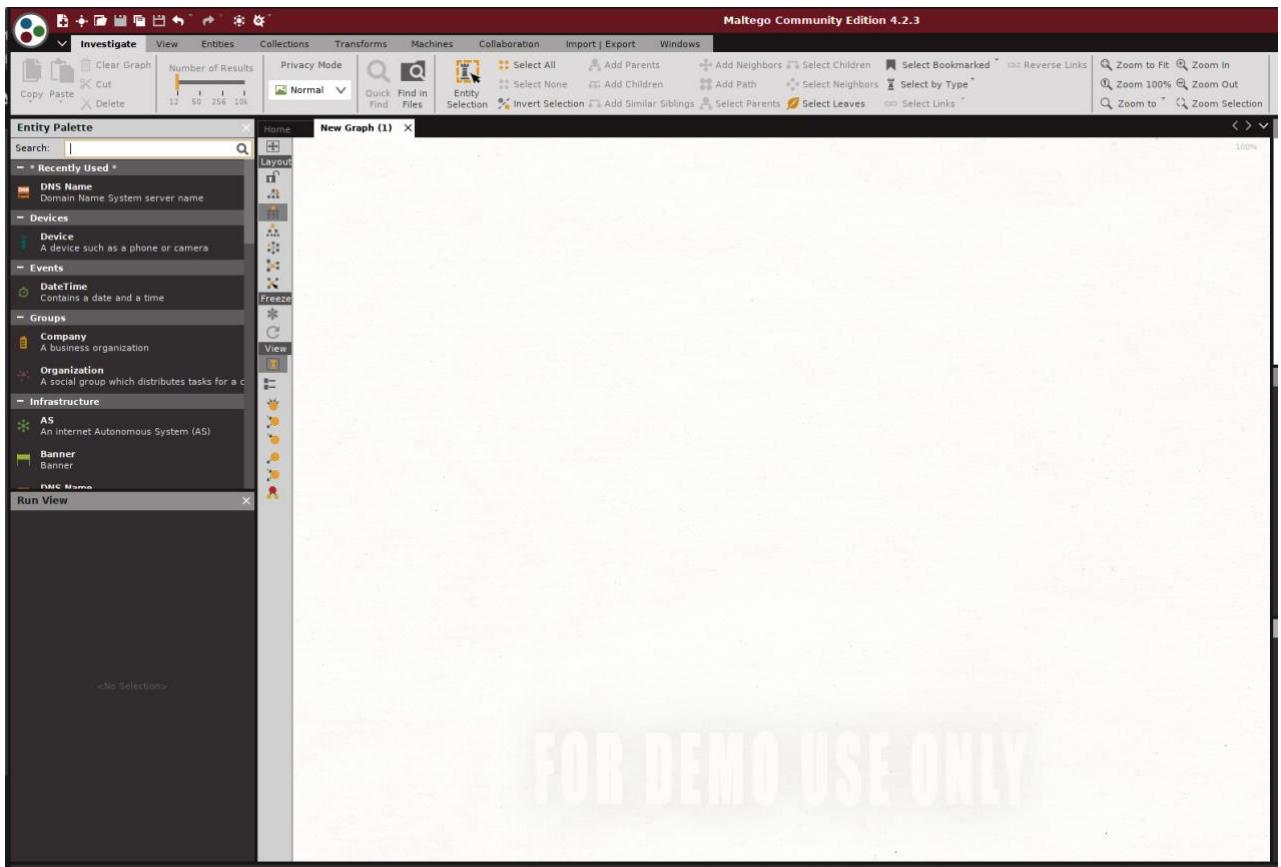
Hộp thoại Ready, chọn “Open a blank graph and let me play around”.



Hình 38. *Hộp thoại Ready thông báo quá trình cài đặt Maltego hoàn tất*

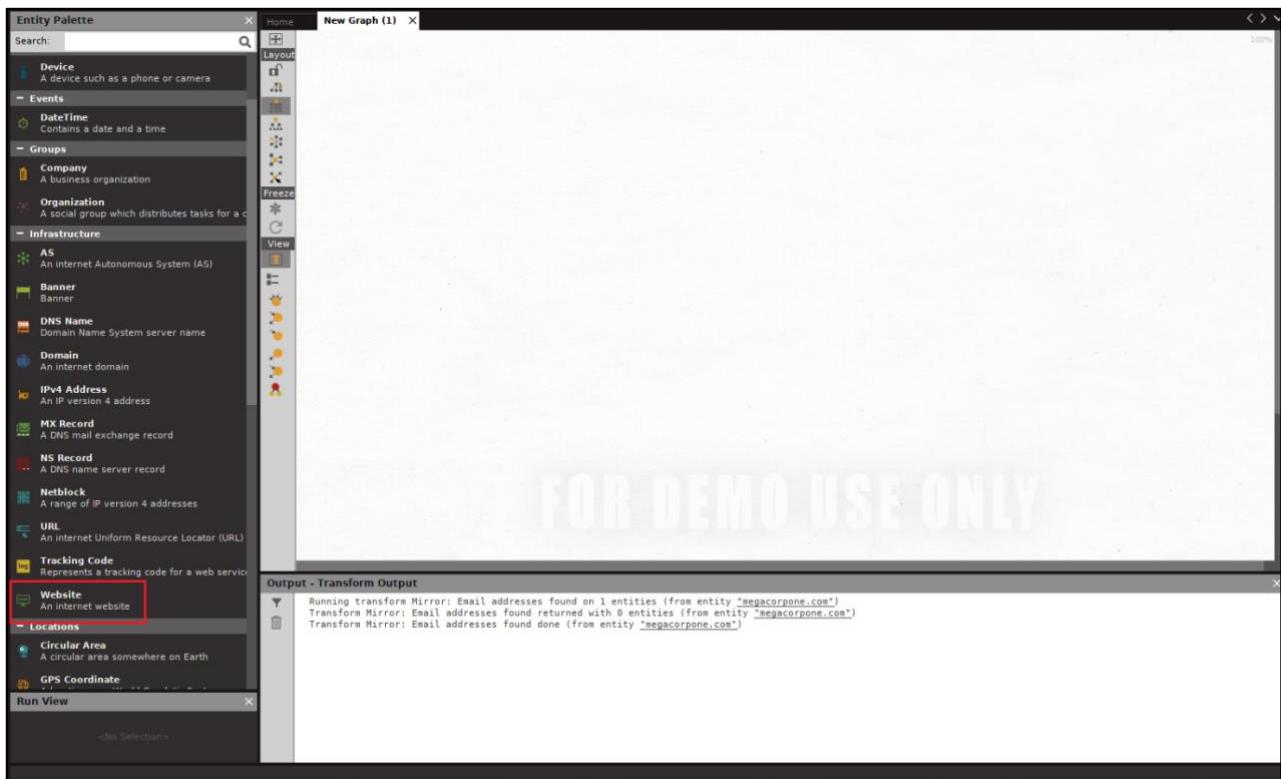
Ở phía bên trái, có một phần có tên là "Entity Pallette" cung cấp nhiều tùy chọn tìm kiếm như vị trí, chi tiết hash của phần mềm độc hại, thông tin về các port của hệ thống, thông tin về dịch vụ mạng, thông tin về địa chỉ Email, v.v. nhiều tùy chọn có sẵn mà bạn có thể sử dụng miễn phí.

Lab 2: Thu thập thông tin



Hình 39. Giao diện Maltego

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



Hình 40. Chọn website và kéo thả vào chính giữa

Thực thể website được xuất hiện, double click vào domain mặc định (www.paterva.com) và sửa thành www.megacorpone.com



Hình 41. *Thay đổi đối tượng cần thu thập thông tin*

Chuột phải vào thực thể này vào chọn All Transforms.



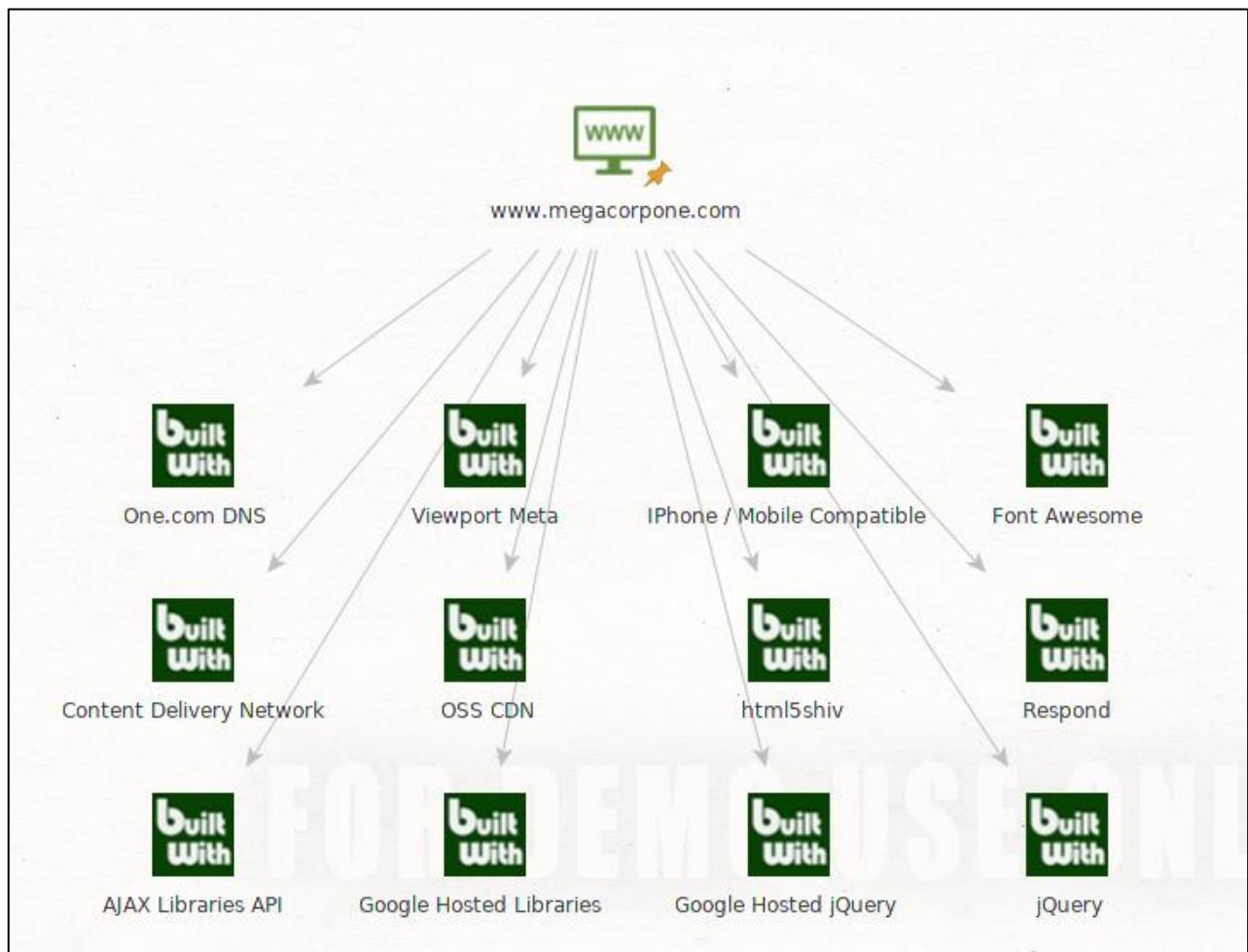
Hình 42. *Chọn All Transforms*

Danh sách các Transforms xuất hiện, chọn To Server Technologies [Using BuiltWith].



Hình 43. Chọn To Server Technologies

Kết quả hiển thị các công nghệ mà website MegaCorp One sử dụng.



Hình 44. Các công nghệ mà MegaCorp One sử dụng

® Bài tập về nhà (Yêu cầu làm)

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

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

j) DNS Enumeration

Hệ thống tên miền (Domain Name System – DNS) là một trong những hệ thống quan trọng nhất trên Internet và là một cơ sở dữ liệu phân tán chịu trách nhiệm chuyển đổi tên miền thành địa chỉ IP.

Tương tác với máy chủ DNS

Mỗi tên miền có thể sử dụng các loại bản ghi DNS khác nhau. Một số bản ghi DNS phổ biến nhất bao gồm:

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

Do có rất nhiều thông tin được chứa bên trong DNS, nó thường là mục tiêu trong giai đoạn thu thập thông tin chủ động.

Sử dụng lệnh **host** để tìm địa chỉ IP của www.megacorpone.com

```
root@kali:~# host www.megacorpone.com
www.megacorpone.com has address 3.220.87.155
```

Hình 45. Sử dụng lệnh host để tìm A record cho tên miền www.megacorpone.com

Mặc định, lệnh **host** sẽ tìm kiếm bản ghi A, nhưng chúng ta có thể yêu cầu các bản ghi khác, như TXT hoặc MX. Sử dụng tùy chọn **-t** để chỉ định loại bản ghi muốn tìm kiếm.

```
root@kali:~# host -t txt megacorpone.com
megacorpone.com descriptive text "Try Harder"
megacorpone.com descriptive text "google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0vWq5pA"
root@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 20 spool.mail.gandi.net.
megacorpone.com mail is handled by 10 fb.mail.gandi.net.
```

Hình 46. Sử dụng lệnh **host** để tìm kiếm các bản ghi TXT và MX cho tên miền *megacorpone.com*

[®] **Bài tập về nhà (Yêu cầu làm)**

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

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

Tra cứu tự động (Automating Lookups)

Bây giờ chúng ta đã thu thập được một số thông tin từ tên miền *megacorpone.com*, chúng ta có thể tiếp tục sử dụng thêm các truy vấn DNS để tìm kiếm các hostname và địa chỉ IP cùng thuộc một tên miền.

Sử dụng lại lệnh **host** đối với máy chủ www.megacorpone.com.

```
root@kali:~# host www.megacorpone.com
www.megacorpone.com has address 3.220.87.155
root@kali:~#
```

Hình 47. Sử dụng lệnh **host** cho hostname hợp lệ

Bây giờ, kiểm tra xem liệu *megacorpone.com* có máy chủ với hostname tên là “noexist”. Theo dõi sự khác nhau giữa các kết quả trả về.

```
root@kali:~# host noexist.megacorpone.com
Host noexist.megacorpone.com not found: 3(NXDOMAIN)
root@kali:~#
```

Hình 48. Sử dụng lệnh **host** cho hostname không hợp lệ

Trong Hình 47, chúng ta đã truy vấn một hostname hợp lệ và đã nhận được địa chỉ phân giải IP tương ứng. Ngược lại, ở Hình 48, kết quả báo lỗi hostname không tìm thấy cho ta biết bản ghi DNS không tồn tại đối với hostname này. Bây giờ chúng ta đã hiểu được cách tìm kiếm các hostname hợp lệ, chúng ta có thể tự động hóa quá trình này.

® Bài tập về nhà (Yêu cầu làm)

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?

Forward Lookup Brute Force

Brute Force là kỹ thuật tìm kiếm thông tin hợp lệ, bao gồm các thư mục trên máy chủ web, các kết hợp username và password, hoặc trong trường hợp này, các bản ghi DNS hợp lệ. Bằng cách sử dụng danh sách chứa các hostname thông dụng, chúng ta có thể sử dụng để đoán các bản ghi DNS và kiểm tra kết quả trả về cho các hostname hợp lệ.

Đầu tiên, tạo danh sách các hostname thường gặp.

```
root@kali:~/Desktop# cat list.txt
www
ftp
mail
owa
proxy
router
admin
www2
firewall
mx
pop3
dns
ca
root@kali:~/Desktop#
```

Hình 49. Danh sách các hostname thông dụng

Sử dụng Bash script để phân giải mỗi hostname có trong danh sách.

```
root@kali:~/Desktop# for ip in $(cat list.txt); do host $ip.megacorpone.com; done
www.megacorpone.com has address 3.220.87.155
Host ftp.megacorpone.com not found: 3(NXDOMAIN)
mail.megacorpone.com has address 3.220.61.179
Host owa.megacorpone.com not found: 3(NXDOMAIN)
Host proxy.megacorpone.com not found: 3(NXDOMAIN)
router.megacorpone.com has address 3.220.61.179
admin.megacorpone.com has address 3.220.61.179
www2.megacorpone.com has address 3.220.61.179
Host firewall.megacorpone.com not found: 3(NXDOMAIN)
Host mx.megacorpone.com not found: 3(NXDOMAIN)
Host pop3.megacorpone.com not found: 3(NXDOMAIN)
Host dns.megacorpone.com not found: 3(NXDOMAIN)
Host ca.megacorpone.com not found: 3(NXDOMAIN)
```

Hình 50. Sử dụng Bash script để brute force forward DNS name

® Bài tập về nhà (Yêu cầu làm)

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

Reverse Lookup Brute Force

Ngoài dãy IP (3.220.X.Y) đã được tìm kiếm ở trên, tổ chức MegaCorp One còn dãy IP 38.100.193.X. Nếu quản trị viên của *megacorpone.com* cấu hình các bản ghi PTR cho teen miền này, chúng ta có thể quét địa chỉ IP trong dãy IP đó để tìm ra hostname thuộc MegaCorp One.

Chúng ta sẽ quét địa chỉ IP từ 38.100.193.50 đến 38.100.193.100. Sử dụng lệnh **grep -v** để loại bỏ các hostname không hợp lệ.

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

Hình 51. Sử dụng Bash script để brute force reverse DNS name

Chúng ta có thể thấy, kết quả cho ta biết thêm các hostname hợp lệ khác như snmp, siem, mail2...

DNS Zone Transfers

Zone Transfer là một bản sao cơ sở dữ liệu giữa các máy chủ DNS liên quan trong đó tập tin zone được sao chép từ máy chủ DNS chính (Master DNS Server) sang máy chủ DNS phụ (Slave DNS Server). Tập tin zone chứa danh sách tất cả các tên DNS được cấu hình cho zone đó. Zone transfer chỉ được cho phép đối với các máy chủ DNS phụ có ủy quyền, nhưng nhiều quản trị viên cấu hình sai các máy chủ DNS và trong trường hợp này, bất kỳ ai yêu cầu bản sao của zone thường sẽ nhận được kết quả trả về.

Điều này chẳng khác nào đưa cho hacker danh sách các tên miền đầy đủ của tổ chức. Tất cả tên, địa chỉ và chức năng của máy chủ có thể bị lộ ra ngoài.

Việc chuyển vùng thành công không trực tiếp dẫn đến rò rỉ thông tin mạng, mặc dù nó là tiền đề, tạo điều kiện thuận lợi cho kẻ xấu.

Cú pháp lệnh **host** thực hiện zone transfer như sau:

```
host -l <domain name> <dns server address>
```

Hình 52. Sử dụng lệnh host để thực hiện DNS zone transfer

Như đã biết ở Hình 5, chúng ta biết được có 3 máy chủ DNS đang quản lý tên miền megacorpone.com: ns1, ns2 và ns3.

Thử thực hiện zone transfer của mỗi máy chủ này. Sử dụng lệnh **host -l** (liệt kê các zone) để thực hiện zone transfer:

```
root@kali:~/Desktop# host -l megacorpone.com ns1.megacorpone.com
Using domain server:
Name: ns1.megacorpone.com
Address: 3.220.61.179#53
Aliases:

Host megacorpone.com not found: 5(REFUSED)
; Transfer failed.
root@kali:~/Desktop#
```

Hình 53. Thực hiện zone transfer ở nameserver ns1 thất bại

Đáng tiếc, nameserver đầu tiên, ns1, không cho phép thực hiện DNS zone transfer, vì vậy chúng ta thất bại. Thực hiện tương tự với nameserver kế tiếp, ns2.

```
root@kali:~/Desktop# host -l megacorpone.com ns2.megacorpone.com
Using domain server:
Name: ns2.megacorpone.com
Address: 3.211.51.86#53
Aliases:

megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
megacorpone.com name server ns3.megacorpone.com.
admin.megacorpone.com has address 3.220.61.179
beta.megacorpone.com has address 3.220.61.179
fs1.megacorpone.com has address 3.220.61.179
intranet.megacorpone.com has address 3.220.61.179
mail.megacorpone.com has address 3.220.61.179
mail2.megacorpone.com has address 3.220.61.179
ns1.megacorpone.com has address 3.220.61.179
ns2.megacorpone.com has address 3.211.51.86
ns3.megacorpone.com has address 3.212.85.86
router.megacorpone.com has address 3.220.61.179
siem.megacorpone.com has address 3.220.61.179
snmp.megacorpone.com has address 3.220.61.179
support.megacorpone.com has address 3.212.85.86
syslog.megacorpone.com has address 3.220.61.179
test.megacorpone.com has address 3.220.61.179
vpn.megacorpone.com has address 3.220.61.179
www.megacorpone.com has address 3.220.87.155
www2.megacorpone.com has address 3.220.61.179
root@kali:~/Desktop#
```

Hình 54. Sử dụng lệnh host để minh họa DNS zone transfer

Nameserver này cho phép zone transfer và cung cấp tập tin zone đầy đủ cho tên miền megacorpone.com, cung cấp danh sách địa chỉ IP và hostname tương ứng.

[®] Bài tập về nhà (Yêu cầu làm)

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.

Các công cụ có liên quan có trên Kali Linux

DNSRecon

DNSRecon là một công cụ được viết bằng Python có nhiệm vụ kiểm tra DNS. Sử dụng tùy chọn **-d** để chỉ định tên miền và **-t** để chỉ định loại enumeration (trong trường hợp này là zone transfer), tạo ra kết quả như sau:

```

root@kali:~/Desktop# dnsrecon -d megacorpone.com -t axfr
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for megacorpone.com name servers
[*] Resolving SOA Record
[+]      SOA ns1.megacorpone.com 3.220.61.179
[*] Resolving NS Records
[*] NS Servers found:
[*]   NS ns1.megacorpone.com 3.220.61.179
[*]   NS ns3.megacorpone.com 3.212.85.86
[*]   NS ns2.megacorpone.com 3.211.51.86
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 3.212.85.86 (111.69.131.142) 56(84) bytes of data.
[+] 3.212.85.86 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: REFUSED (written, 0 received, 500K packet loss, time 0ms)
Traceback (most recent call last):
  File "/usr/share/dnsrecon/lib/dnshelper.py", line 429, in zone_transfer
    zone = self.from_wire(dns.query.xfr(ns_srv, self._domain))
          ^_____
  File "/usr/share/dnsrecon/lib/dnshelper.py", line 361, in from_wire
    for r in xfr:
      File "/usr/lib/python3/dist-packages/dns/query.py", line 627, in xfr
        raise TransferError(rcode)
dns.query.TransferError: Zone transfer error: REFUSED
[*]
[*] Trying NS server 3.220.61.179
[+] 3.220.61.179 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] Zone transfer error: REFUSED
Traceback (most recent call last):
  File "/usr/share/dnsrecon/lib/dnshelper.py", line 429, in zone_transfer
    zone = self.from_wire(dns.query.xfr(ns_srv, self._domain))
          ^_____
  File "/usr/share/dnsrecon/lib/dnshelper.py", line 361, in from_wire
    for r in xfr:
      File "/usr/lib/python3/dist-packages/dns/query.py", line 627, in xfr
        raise TransferError(rcode)
dns.query.TransferError: Zone transfer error: REFUSED
[*]
[*] Trying NS server 3.211.51.86
[+] 3.211.51.86 Has port 53 TCP Open
[+] Zone Transfer was successful!!
[*]   NS ns1.megacorpone.com 3.220.61.179
[*]   NS ns2.megacorpone.com 3.211.51.86
[*]   NS ns3.megacorpone.com 3.212.85.86
[*]   TXT Try Harder
[*]   TXT google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfcJ32hMNV3GtC0wWq5pA
[*]   MX @.megacorpone.com fb.mail.gandi.net 217.70.178.217
[*]   MX @.megacorpone.com spool.mail.gandi.net 217.70.178.1
[*]   A admin.megacorpone.com 3.220.61.179
[*]   A beta.megacorpone.com 3.220.61.179
[*]   A fs1.megacorpone.com 3.220.61.179
[*]   A intranet.megacorpone.com 3.220.61.179
[*]   A mail.megacorpone.com 3.220.61.179
[*]   A mail2.megacorpone.com 3.220.61.179
[*]   A ns1.megacorpone.com 3.220.61.179
[*]   A ns2.megacorpone.com 3.211.51.86
[*]   A ns3.megacorpone.com 3.212.85.86
[*]   A router.megacorpone.com 3.220.61.179
[*]   A siem.megacorpone.com 3.220.61.179
[*]   A snmp.megacorpone.com 3.220.61.179
[*]   A

```

Hình 55. Sử dụng dnsrecon để thực hiện zone transfer

Dựa vào kết quả trả về, ta có thể thực hiện DNS zone transfer đối với tên miền megacorpone.com.

Bây giờ, thực hiện brute force các hostname khác sử dụng tập tin **list.txt** đã được tạo từ trước (Hình 49). Sử dụng tùy chọn **-d** để chỉ định tên miền, **-D** để chỉ định tên tập tin chứa các subdomain có thể, và **-t** để chỉ định loại enumeration để thực hiện (ở đây là **brt**).

```

root@kali:~/Desktop# cat list.txt
www
ftp
mail
owa a.ovpn
proxy
router
admin
www2
firewall
mx test.html.jpg
pop3
dns
ca

root@kali:~/Desktop# dnsrecon -d megacorpone.com -D ~/Desktop/list.txt -t brt
[*] Performing host and subdomain brute force against megacorpone.com ta...
[+] mail.megacorpone.com: A : 3.220.61.179
[+] www.megacorpone.com: A : 3.220.87.155
[+] router.megacorpone.com: A : 3.220.61.179
[+] www2.megacorpone.com: A : 3.220.61.179
[+] admin.megacorpone.com: A : 3.220.61.179
[+] 5 Records Found
root@kali:~/Desktop#

```

Hình 56. Brute force hostname sử dụng DNSRecon

® Bài tập về nhà (Cộng điểm)

26. Viết *Liệt kê danh sách các loại enumeration có thể được sử dụng cùng với 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)

DNSEnum

DNSEnum là một công cụ kiểm tra DNS phổ biến khác. Cũng tương tự DNSRecon, DNSEnum cũng thực hiện được các chức năng tương tự như brute force, zone transfer...

```

root@kali:~/Desktop# dnsenum megacorpone.com
dnsenum VERSION:1.2.6

----- megacorpone.com -----

Host's addresses: --- uit.edu.vn ping statistics ---
  1 packets transmitted, 0 received, 100% packet loss, time 0ms

Name Servers: --- uit.edu.vn ping statistics ---
  1 packets transmitted, 0 received, 100% packet loss, time 0ms

ns3.megacorpone.com.      5      IN   A      3.212.85.86
ns2.megacorpone.com.      5      IN   A      3.211.51.86
ns1.megacorpone.com.      5      IN   A      3.220.61.179
                                         PING uit.edu.vn (118.69.123.142) 56(84) bytes of data.

Mail (MX) Servers: --- uit.edu.vn ping statistics ---
  1 packets transmitted, 0 received, 100% packet loss, time 0ms

fb.mail.gandi.net.        5      IN   A      217.70.178.217
mail.megacorpone.com.     5      IN   A      3.220.61.179
spool.mail.gandi.net.    5      IN   A      217.70.178.1
mail2.megacorpone.com.    5      IN   A      3.220.61.179
                                         PING uit.edu.vn ping statistics
                                         1 packets transmitted, 0 received, 100% packet loss, time 101ms

Trying Zone Transfers and getting Bind Versions:
----- ns3.megacorpone.com -----
Trying Zone Transfer for megacorpone.com on ns3.megacorpone.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for megacorpone.com on ns2.megacorpone.com ...
megacorpone.com.          259200  IN   SOA      ( "Try
megacorpone.com.          259200  IN   TXT      ( "Try
megacorpone.com.          259200  IN   TXT      ( "Try
megacorpone.com.          259200  IN   MX      10
megacorpone.com.          259200  IN   MX      20
megacorpone.com.          259200  IN   MX      50
megacorpone.com.          259200  IN   MX      60
megacorpone.com.          259200  IN   NS      ns1.megacorpone.com.
megacorpone.com.          259200  IN   NS      ns2.megacorpone.com.
megacorpone.com.          259200  IN   NS      ns3.megacorpone.com.
admin.megacorpone.com.    259200  IN   A       3.220.61.179
beta.megacorpone.com.    259200  IN   A       3.220.61.179
fs1.megacorpone.com.     259200  IN   A       3.220.61.179
intranet.megacorpone.com. 259200  IN   A       3.220.61.179
mail.megacorpone.com.     259200  IN   A       3.220.61.179
mail2.megacorpone.com.    259200  IN   A       3.220.61.179
ns1.megacorpone.com.     259200  IN   A       3.220.61.179
ns2.megacorpone.com.     259200  IN   A       3.211.51.86
ns3.megacorpone.com.     259200  IN   A       3.212.85.86
router.megacorpone.com.   259200  IN   A       3.220.61.179
siem.megacorpone.com.    259200  IN   A       3.220.61.179
snmp.megacorpone.com.    259200  IN   A       3.220.61.179
support.megacorpone.com. 259200  IN   A       3.212.85.86
syslog.megacorpone.com.  259200  IN   A       3.220.61.179
test.megacorpone.com.    259200  IN   A       3.220.61.179
vpn.megacorpone.com.     259200  IN   A       3.220.61.179
www.megacorpone.com.     259200  IN   A       3.220.87.155
www2.megacorpone.com.    259200  IN   A       3.220.61.179

```

Hình 57. Sử dụng công cụ DNSEnum cho tên miền megacorpone.com

® Bài tập về nhà (Cộng điểm)

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?

k) Port Scanning

Port Scanning là quá trình kiểm tra các port TCP hoặc UDP trên máy từ xa với mục đích phát hiện những dịch vụ đang chạy trên máy mục tiêu và những khả năng tấn công tiềm ẩn ứng với các dịch vụ đó.

Điều cần thiết là phải hiểu ý nghĩa của việc scan port, cũng như ảnh hưởng khi thực hiện việc scan port. Do số lượng lưu lượng truy cập mà một số quá trình quét có thể tạo ra, cùng với tính chất xâm nhập của chúng, việc scan port một cách “mù quáng” có thể gây ra các tác động xấu đến hệ thống mục tiêu hoặc mạng khách hàng như làm quá tải máy chủ và liên kết mạng hoặc làm kích hoạt IDS. Việc scan sai có thể dẫn đến downtime cho khách hàng.

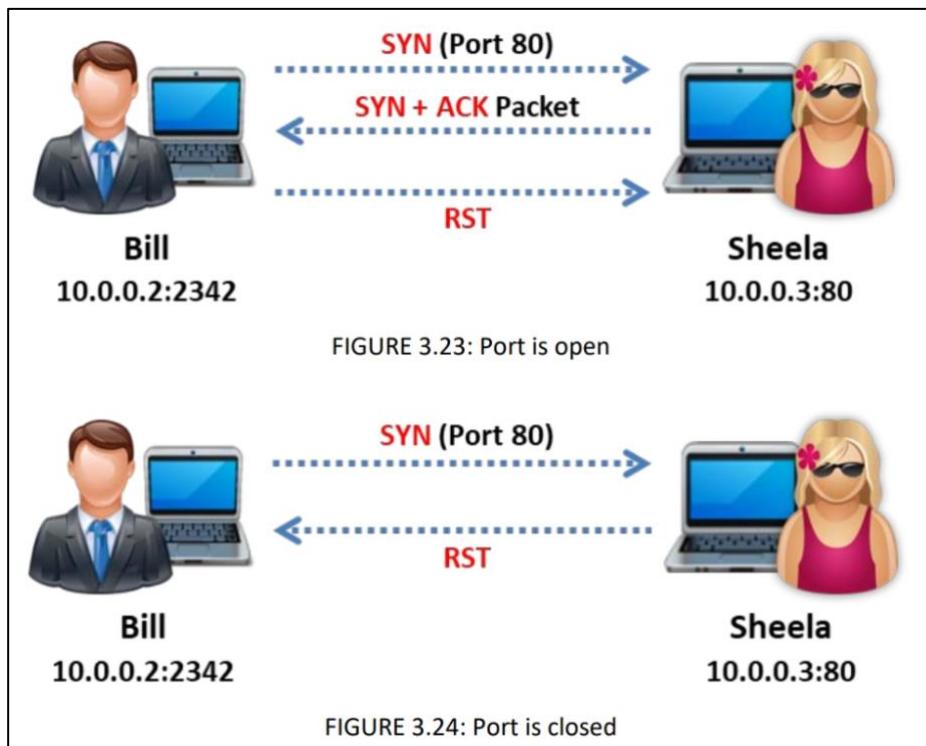
Port Scanning sử dụng Nmap

Nmap (viết bởi Gordon Lyon, hay còn gọi là Fyodor) là một trong những công cụ scan port phổ biến, linh hoạt và mạnh mẽ nhất hiện nay. Nó đã được phát triển tích cực trong hơn một thập kỷ và có nhiều tính năng ngoài chức năng scan port đơn thuần.

Stealth/SYN Scanning

Kỹ thuật quét ưa thích của Nmap là SYN, hay còn gọi là quét "stealth". Có nhiều lợi ích khi sử dụng SYN scan và do đó, nó là kỹ thuật quét mặc định được sử dụng khi không có kỹ thuật quét nào được chỉ định trong lệnh nmap.

SYN scanning là phương thức scan port TCP bằng cách gửi các gói tin SYN đến các port khác nhau trên máy mục tiêu mà không thực hiện quá trình bắt tay ba bước hoàn thiện. Nếu port TCP đó mở, SYN-ACK sẽ được gửi về từ máy mục tiêu, cho ta biết port đang mở. Tại thời điểm đó, Nmap sẽ không quan tâm đến việc gửi gói tin ACK để hoàn tất quá trình bắt tay ba bước.



Hình 58. TCP SYN Scan

```
root@kali:~/Desktop# sudo nmap -sS 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 12:31 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0051s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp    -- uit.edu.vn ping statistics ---
22/tcp    open  ssh    1 packets transmitted, 0 received, 100% packet loss, time 0ms
23/tcp    open  telnet
25/tcp    open  smtp   root@kali:~# ping uit.edu.vn
53/tcp    open  domain
53/tcp    open  domain
80/tcp    open  http   C
111/tcp   open  rpcbind uit.edu.vn ping statistics ---
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec   root@kali:~#
513/tcp   open  login   root@kali:~# ping uit.edu.vn
514/tcp   open  shell   NG uit.edu.vn (118.69.123.142) 56(84) bytes of data.
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs    1 packets transmitted, 0 received, 100% packet loss, time 0ms
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql  root@kali:~# ping uit.edu.vn
5432/tcp  open  postgresql
5900/tcp  open  vnc    C
6000/tcp  open  X11   -- uit.edu.vn ping statistics ---
6667/tcp  open  irc    2 packets transmitted, 0 received, 100% packet loss, time 1013ms
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
root@kali:~/Desktop#
```

Hình 59. Sử dụng Nmap để thực hiện SYN scan

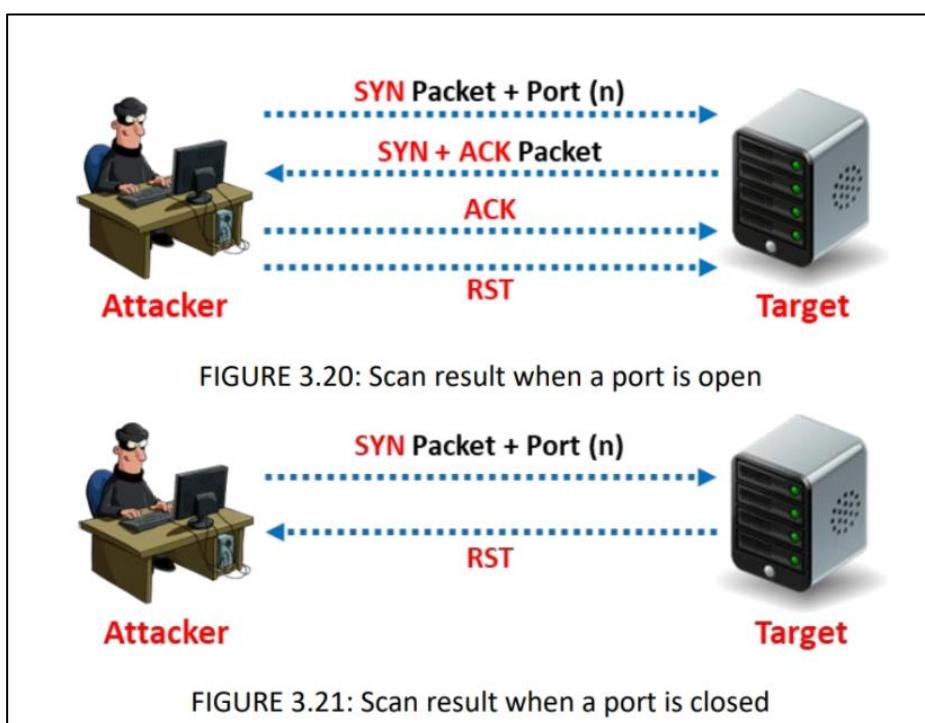
Bởi vì quá trình bắt tay ba bước chưa hoàn thành, thông tin sẽ không được chuyển đến tầng ứng dụng và kết quả là, sẽ không xuất hiện trong bất kỳ log của ứng dụng nào. SYN Scan cũng nhanh hơn và hiệu quả hơn vì ít gói tin được gửi và nhận hơn.

[®] **Bài tập về nhà (Yêu cầu làm)**

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

TCP Connect Scanning

Khác với TCP SYN Scan, TCP Connect Scan hoàn tất quá trình bắt tay ba bước với máy mục tiêu. Sau khi nhận gói tin SYN-ACK từ máy mục tiêu, Nmap sẽ thực hiện gửi lại gói tin ACK để hoàn tất việc kết nối. Một khi quá trình bắt tay ba bước hoàn tất, Nmap sẽ gửi gói tin RST để kết thúc kết nối.



Hình 60. *TCP Connect Scan*

```

root@kali:~/Desktop# nmap -sT 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 12:44 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0029s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp   -- uit.edu.vn ping statistics ---
22/tcp    open  ssh   1 packets transmitted, 0 received, 100% packet loss, time 0ms
23/tcp    open  telnet
25/tcp    open  smtp  root@kali:~# ping uit.edu.vn
53/tcp    open  domain G uit.edu.vn (118.69.123.142) 56(84) bytes of data.
80/tcp    open  http  C
111/tcp   open  rpcbind uit.edu.vn ping statistics ---
139/tcp   open  netbios-ssn s transmitted, 0 received, 100% packet loss, time 0ms
445/tcp   open  microsoft-ds
512/tcp   open  exec  root@kali:~#
513/tcp   open  login root@kali:~# ping uit.edu.vn
514/tcp   open  shell  uit.edu.vn (118.69.123.142) 56(84) bytes of data.
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock .edu.vn ping statistics ---
2049/tcp  open  nfs   1 packets transmitted, 0 received, 100% packet loss, time 0ms
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql root@kali:~# ping uit.edu.vn
5432/tcp  open  postgresql uit.edu.vn (118.69.123.142) 56(84) bytes of data.
5900/tcp  open  vnc   ^C
6000/tcp  open  X11   -- uit.edu.vn ping statistics ---
6667/tcp  open  irc   2 packets transmitted, 0 received, 100% packet loss, time 1013ms
8009/tcp  open  ajp13
8180/tcp  open  unknown root@kali:~#
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
root@kali:~/Desktop#

```

Hình 61. Sử dụng Nmap để thực hiện TCP Connect Scan

[®] **Bài tập về nhà (Yêu cầu làm)**

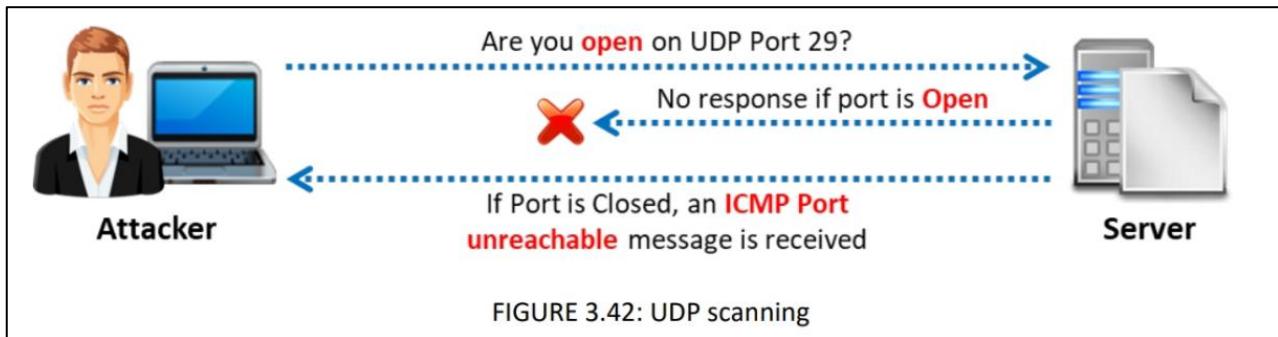
30. Thực hiện bắt Wireshark để mô tả cách gói tin được gửi và nhận khi thực hiện TCP Connect Scan sử dụng Nmap.

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...)

UDP Scanning

Không có quá trình bắt tay ba bước khi thực hiện quét UDP. Giao thức UDP có thể khó sử dụng hơn so với quét TCP vì khi gửi gói tin đến máy mục tiêu, bạn không thể xác định máy chủ còn sống (alive), chết (dead) hay đã được lọc (filtered). Tuy nhiên, bạn có thể sử dụng một gói tin ICMP để kiểm tra các port mở hoặc đóng. Nếu bạn gửi một gói UDP đến một port mà không có ứng dụng nào sử dụng, IP stack sẽ trả về một gói tin “ICMP port unreachable”. Nếu bất kỳ cổng nào trả về lỗi ICMP, chứng tỏ cổng đó đang

đóng, còn nếu không có bất kỳ phản hồi nào, chứng tỏ cổng đó đang mở hoặc đang bị lọc thông qua firewall.



Hình 62. *UDP Scanning*

```
root@kali:~/Desktop# sudo nmap -sU 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:01 EDT
Stats: 0:06:27 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 38.28% done; ETC: 13:18 (0:10:26 remaining)
Nmap scan report for 192.168.111.150
Host is up (0.00066s latency).
Not shown: 994 closed ports
          edu.vn ping statistics ---
PORT      STATE      1 paSERVICEtransmitted, 0 received, 100% packet loss, time 0ms
53/udp    open       domain
69/udp    open|filtered tftp :# ping uit.edu.vn
111/udp   open       PING rpcbind uit.edu.vn (118.69.123.142) 56(84) bytes of data.
137/udp   open       ^C netbios-ns
138/udp   open|filtered netbios-dgmping statistics ---
2049/udp  open       1 paNFS transmitted, 0 received, 100% packet loss, time 0ms
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1070.82 seconds
root@kali:~/Desktop#
```

Hình 63. *Sử dụng Nmap để thực hiện UDP Scan*

UDP Scan (-sU) có thể được sử dụng cùng với TCP SYN Scan (-sS) để tạo nên một bức tranh hoàn thiện đối với máy mục tiêu.

```
root@kali:~/Desktop# sudo nmap -sS -sU 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:20 EDT
Nmap scan report for 192.168.111.150
Host is up (0.00072s latency).
Not shown: 1925 closed ports, 48 open|filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
2049/udp  open  nfs
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

Hình 64. Sử dụng Nmap thực hiện quét kết hợp UDP và SYN scan

Network Sweeping

Để xử lý số lượng lớn máy chủ hoặc để cố gắng duy trì lưu lượng mạng, chúng ta có thể cố gắng thăm dò mục tiêu bằng kỹ thuật Network Sweeping, trong đó chúng ta bắt đầu bằng cách scan rộng và sử dụng các lần scan cụ thể hơn đối với các máy chủ cần quan tâm.

Khi thực hiện Network Sweeping với Nmap bằng cách sử dụng tùy chọn **-sn**, quá trình khám phá máy chủ không chỉ bao gồm việc gửi một gói tin ICMP echo request. Một số đầu dò khác được sử dụng cùng với ICMP request. Nmap cũng gửi một gói TCP SYN đến port 443, một gói TCP ACK đến port 80 và một ICMP timestamp request để xác minh xem máy chủ có sẵn hay không.

```
root@kali:~# nmap -sn 192.168.111.1-254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:14 EDT
Nmap scan report for 192.168.111.1
Host is up (0.00055s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.00017s latency).
MAC Address: 00:50:56:E5:A6:14 (VMware)
Nmap scan report for 192.168.111.150
Host is up (0.00027s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.111.254
Host is up (0.00014s latency).
MAC Address: 00:50:56:E4:1A:EA (VMware)
Nmap scan report for 192.168.111.131
Host is up.
Nmap done: 254 IP addresses (5 hosts up) scanned in 1.77 seconds
root@kali:~#
```

Hình 65. Sử dụng nmap để thực hiện Network Sweep

Sử dụng tham số **-oG** để lưu kết quả ra định dạng có thể dễ dàng quản lý, tìm kiếm.

```
root@kali:~# nmap -v -sn 192.168.111.1-254 -oG ping-sweep.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:17 EDT
Initiating ARP Ping Scan at 13:17
Scanning 253 hosts [1 port/host]
Completed ARP Ping Scan at 13:17, 1.97s elapsed (253 total hosts)
Initiating Parallel DNS resolution of 253 hosts. at 13:17
Completed Parallel DNS resolution of 253 hosts. at 13:17, 0.00s elapsed
Nmap scan report for 192.168.111.1
Host is up (0.0017s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.00016s latency).
MAC Address: 00:50:56:E5:A6:14 (VMware)
Nmap scan report for 192.168.111.3 [host down]
Nmap scan report for 192.168.111.4 [host down]
Nmap scan report for 192.168.111.5 [host down]
Nmap scan report for 192.168.111.6 [host down]
Nmap scan report for 192.168.111.7 [host down]
Nmap scan report for 192.168.111.8 [host down]
Nmap scan report for 192.168.111.9 [host down]
Nmap scan report for 192.168.111.10 [host down]
Nmap scan report for 192.168.111.11 [host down]
Nmap scan report for 192.168.111.12 [host down]
Nmap scan report for 192.168.111.13 [host down]
```

Hình 66. Sử dụng nmap để thực hiện Network Sweep và lưu kết quả vào tập tin

Sau đó, sử dụng lệnh **grep** để lấy ra danh sách các host đang hoạt động.

```
root@kali:~# grep Up ping-sweep.txt | cut -d " " -f 2
192.168.111.1
192.168.111.2
192.168.111.150
192.168.111.254
192.168.111.131
root@kali:~# sudo nmap -sS -sU 192.168.111.150
[+] Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:20 EDT
```

Hình 67. Sử dụng lệnh grep để tìm kiếm các host đang hoạt động

Chúng ta cũng có thể quét các cổng TCP hoặc UDP cụ thể trên toàn mạng, thăm dò các dịch vụ và port phổ biến, trong nỗ lực xác định vị trí các hệ thống có thể hữu ích hoặc có các lỗ hổng đã biết. Thực hiện scan này có xu hướng chính xác hơn ping sweep.

```
root@kali:~# nmap -p 80 192.168.111.1-254 -oG web-sweep.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:29 EDT
Nmap scan report for 192.168.111.1
Host is up (0.0014s latency).

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

Nmap scan report for 192.168.111.2
Host is up (0.00018s latency).

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 00:50:56:E5:A6:14 (VMware)

Nmap scan report for 192.168.111.150
Host is up (0.00022s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap scan report for 192.168.111.254
Host is up (0.00038s latency).

PORT      STATE SERVICE
80/tcp    filtered http
MAC Address: 00:50:56:E4:1A:EA (VMware)
```

Hình 68. Chỉ quét port 80 trên toàn mạng

Sau đó, sử dụng lệnh **grep** để lấy ra danh sách các host đang hoạt động và đang mở port 80.

```
root@kali:~# grep open web-sweep.txt | cut -d " " -f 2
192.168.111.150
192.168.111.131
root@kali:~#
```

Hình 69. Chỉ hiển thị các host đang mở port 80 trong toàn mạng

[®] **Bài tập về nhà (Cộng điểm)**

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

OS Fingerprinting

Nmap được tích hợp sẵn một tính năng gọi là OS Fingerprinting (tham số **-O**). Tính năng này cố gắng đoán hệ điều hành cơ bản, bằng cách kiểm tra các gói nhận được từ mục tiêu. Các hệ điều hành khác nhau thường có TCP/IP stack hơi khác nhau, chẳng hạn như giá trị TTL mặc định và TCP window size. Những khác biệt nhỏ này tạo ra một dấu vân tay thường có thể được nhận dạng bởi Nmap. Nmap sẽ kiểm tra lưu lượng mạng gửi và nhận từ máy mục tiêu, đồng thời cố gắng nhận dạng hệ điều hành với một danh sách đã biết.

```

root@kali:~/Desktop# sudo nmap -O 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 13:46 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
root@kali:~/Desktop#

```

Hình 70. Sử dụng Nmap để xác định hệ điều hành của máy mục tiêu

Banner Grabbing/Service Enumeration

Chúng ta có thể xác định các dịch vụ đang chạy trên các port được chỉ định bằng cách kiểm tra các banner của dịch vụ (-sV) và chạy các script khám phá hệ điều hành và dịch vụ (-A).

Tuy nhiên, lưu ý rằng banner có thể được chỉnh sửa bởi quản trị viên. Do đó, chúng có thể được cố ý đặt tên thành dịch vụ giả mạo để đánh lừa kẻ tấn công.

```
root@kali:~# nmap -sV -sT -A 192.168.111.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 10:30 EDT
Nmap scan report for 192.168.111.150
Host is up (0.12s latency).
Not shown: 977 closed ports
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 192.168.111.131
|   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:cf:e1: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)
```

Hình 71. Sử dụng nmap để khám phá các dịch vụ, thu thập thông tin banner

[®] Bài tập về nhà (Yêu cầu làm)

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

Nmap Scripting Engine (NSE)

Chúng ta có thể sử dụng Nmap Scripting Engine (NSE) để khởi chạy các đoạn script do người dùng tạo ra nhằm tự động hóa các tác vụ quét khác nhau. Các script này thực hiện một loạt chức năng bao gồm DNS enumeration, các loại tấn công brute force, và thậm chí là xác định lỗ hổng bảo mật. Các tập lệnh NSE nằm trong thư mục `/usr/share/nmap/scripts`.

Ví dụ, sử dụng `smb-os-discovery` để thử kết nối tới dịch vụ SMB trên máy mục tiêu nhằm xác định hệ điều hành của nó.

```

root@kali:~# nmap 192.168.111.150 --script=smb-os-discovery
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-28 10:42 EDT
Nmap scan report for 192.168.111.150
Host is up (0.0025s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Host script results:
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2020-09-28T10:42:26-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
root@kali:~#

```

Hình 72. Sử dụng nmap NSE để xác định hệ điều hành

® Bài tập về nhà (Yêu cầu làm)

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

C. YÊU CẦU & ĐÁNH GIÁ

1. Yêu cầu

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Có thể thực hiện theo nhóm (4 tối đa sinh viên/nhóm). Đăng ký nhóm cố định từ buổi 1.
- Sinh viên báo cáo kết quả thực hiện và nộp bài bằng **1 trong 2 hình thức**:

I) Báo cáo chi tiết:

Báo cáo cụ thể quá trình thực hành (có ảnh minh họa các bước) và giải thích các vấn đề kèm theo. Trình bày trong file PDF theo mẫu có sẵn tại website môn học.

m) Video trình bày chi tiết:

Quay lại quá trình thực hiện Lab của sinh viên kèm thuyết minh trực tiếp mô tả và giải thích quá trình thực hành. Upload lên **Youtube** và chèn link vào đầu báo cáo theo mẫu. **Lưu ý:** *Không chia sẻ ở chế độ Public trên Youtube.*

Đặt tên file báo cáo theo định dạng như mẫu:

[Mã lớp]-LabX_GroupX

Ví dụ: *[NT101.I11.1]-Lab1_Group2.*

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

2. Đánh giá:

- Sinh viên hiểu và tự thực hiện được bài thực hành, đóng góp tích cực tại lớp.
- Báo cáo trình bày chi tiết, giải thích các bước thực hiện và chứng minh được do nhóm sinh viên thực hiện.
- Hoàn tất nội dung cơ bản và có thực hiện nội dung *mở rộng - cộng điểm* (với lớp ANTN).

Kết quả thực hành cũng được đánh giá bằng kiểm tra kết quả trực tiếp tại lớp vào cuối buổi thực hành hoặc vào buổi thực hành thứ 2.

Lưu ý: *Bài sao chép, nộp trễ, “gánh team”, ... sẽ được xử lý tùy mức độ.*

HẾT

Chúc các bạn hoàn thành tốt!