



# RECONOCIMIENTO DEL OBJETIVO

## ETHICAL HACKING

### MALTEGO EN KALI LINUX

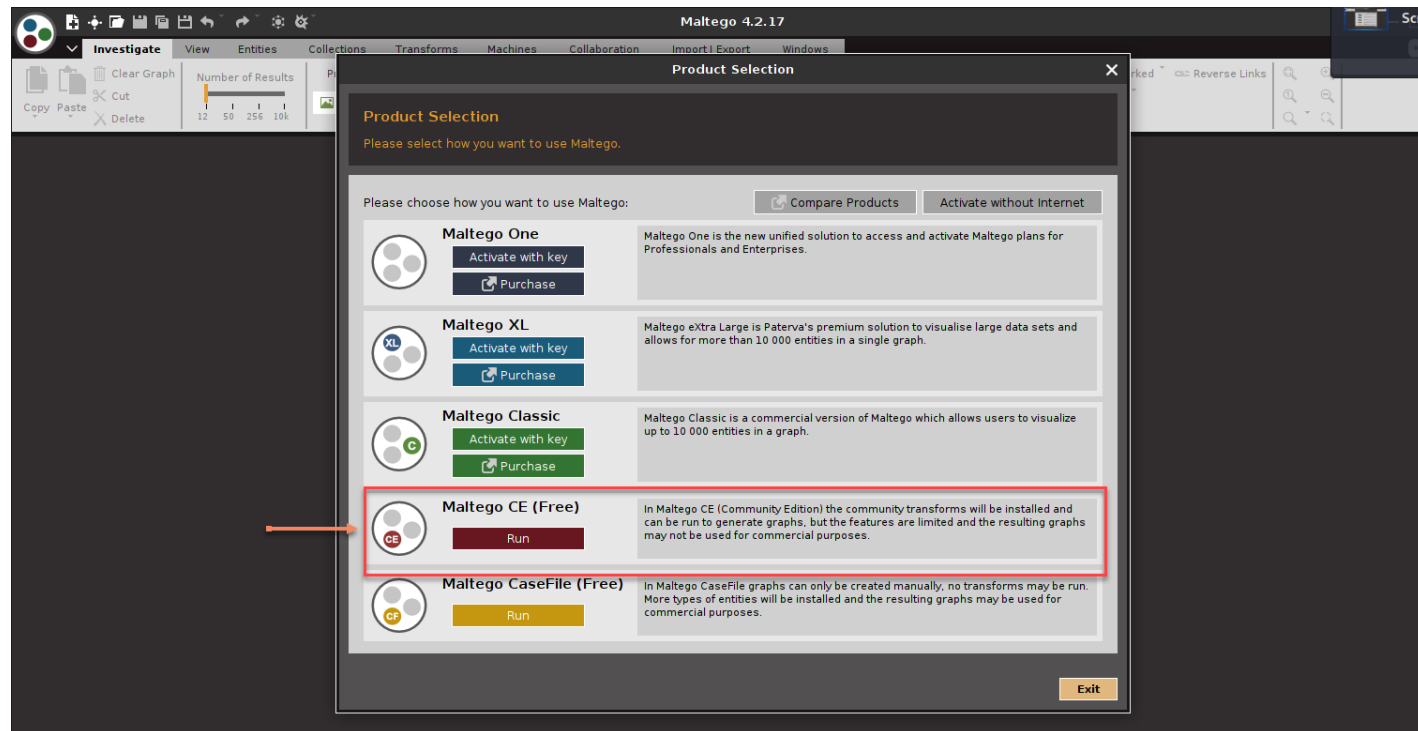


Recopilación de Información  
Minería de Datos





# 1. Configuración de Maltego





## 2. Configuración de Maltego



**Configure Maltego**

**STEPS**

1. **License Agreement**
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready

**LICENSE AGREEMENT: Please read and accept the following License Agreement.**

**General Terms and Conditions  
for Software License Agreements of Paterva  
(Effective 1 September 2020)**

These General Terms and Conditions apply to all licenses (hereinafter referred to as "**Software Licenses**") of Software Products (hereinafter referred to as "**Software**") which are issued by Paterva (Pty) Ltd. (incorporated in South Africa under registration number 2008/005705/07), (hereinafter referred to as "**Licensor**") to its customers (hereinafter referred to as "**Licensee**") (Licensor and Licensee also referred to as "**Party**" and collectively the "**Parties**"). Software subject to these General Terms and Conditions is the intellectual property of the Licensor and/or Maltego Technologies GmbH, registered in the district court Munich, Germany under no. HRB 236523 ("**Maltego**"). To the extent that Software is owned by Maltego, the Licensor has sufficient rights to license same to the Licensee.

**1. Contractual Object**

1.1. These General Terms and Conditions govern the Software Licenses issued to the Licensee by the Licensor by way of a **Software License Agreement**. Sec. 3 specifies the scope of each Software License subscribed regarding the specific Software being licensed as well as the content, location, time and extent of the user rights.

1.2. The number of subscribed Software Licenses and the software components to which the Licenses refer are specified in the Electronic Delivery Document (sec. 2.2.) issued by the Licensor to the Licensee.

☐ **Accept**

**i** Please accept the License Agreement to continue

**< Back** **Next >** **Finish** **Cancel**





### 3. Configuración de Maltego



**Configure Maltego**

**STEPS**

1. License Agreement
2. **Login**
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready

LOGIN: Please log in to use the free online version of Maltego.


Enter your details below to log in to the Maltego Community Server

Or if you have not done so yet, [register here](#)

Login

\* Email Address

Password



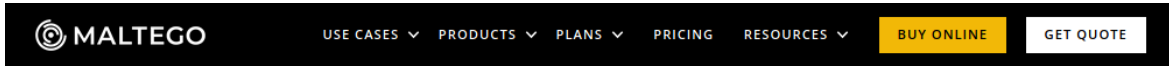
\* Solve captcha

< Back   Next >   Finish   Cancel





## 4. Configuración de Maltego



### Register a Maltego CE Account

Welcome to the Maltego Community Edition page, here you will be able to register an account that you can use with the latest community edition of Maltego!

FIRST NAME \*

e.g. Howard

LAST NAME \*

e.g. Johnson

EMAIL \*

Please note that the activation link for your Maltego account will be sent over email. Please provide a valid email address to proceed further.

e.g. howard.johnson@mail.com

PASSWORD \*

\*\*\*

REPEAT PASSWORD \*

\*\*\*

Already registered? Download your client [here](#) or Login directly in the client.

Forgot password? Reset your password [here](#).

☐ I'm not a robot

reCAPTCHA  
Privacy - Terms

REGISTER

[Paterva Data Privacy Policy](#)





## 5. Configuración de Maltego

### Confirmación de la cuenta de Maltego CE

 Traducido de: Inglés [Mostrar mensaje original](#) | [Activar la traducción automática](#) ⓘ



**Maltego** Support <support@maltego.com>

Mar 10/08/2021 00:24

Para: Usted



**ACTIVA TU CUENTA DE MALTEGO  
CE**

Querido Juan,

Gracias por registrarse en la Edición de la Comunidad de **Maltego**. Para activar su cuenta, haga clic en este enlace:

<https://www.maltego.com/ce-user-activate?code=6a749b77-52c2-4c21-96ee-307244da723f/>



Para obtener más información sobre las nuevas funciones y actualizaciones de productos, consulte <https://www.maltego.com/blog/>.

Para empezar, echa un vistazo a nuestra [documentación](#), [tutoriales](#) y nuestra nueva serie de videos para principiantes - [Maltego Essentials](#).

Saludos cordiales,  
El equipo de **Maltego**





## 6. Configuración de Maltego



**Configure Maltego**

**STEPS**

1. License Agreement
2. **Login**
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options
7. Privacy Mode Options
8. Ready

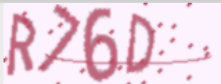
**LOGIN:** Please log in to use the free online version of Maltego.

Enter your details below to log in to the Maltego Community Server  
Or if you have not done so yet, [register here](#)

**Login**

\* **Email Address**  1

**Password**  2



\* **Solve captcha**  3

< Back   Next >   Finish   Cancel





## 7. Configuración de Maltego

**Configure Maltego**

LOGIN RESULT: Please log in to use the free online version of Maltego.

**STEPS**

1. License Agreement
2. Login
3. **Login Result**
4. Install Transforms
5. Help Improve Maltego
6. Web Browser Options

**Hello Juan, welcome to Maltego Community Edition!**

Personal details

First name	<b>Juan</b>
Surname	<b>Muller</b>
Email address	<b>jmullert@senati.pe</b>

Your API key is valid until September 3, 2021 at 12:00:00 AM EDT

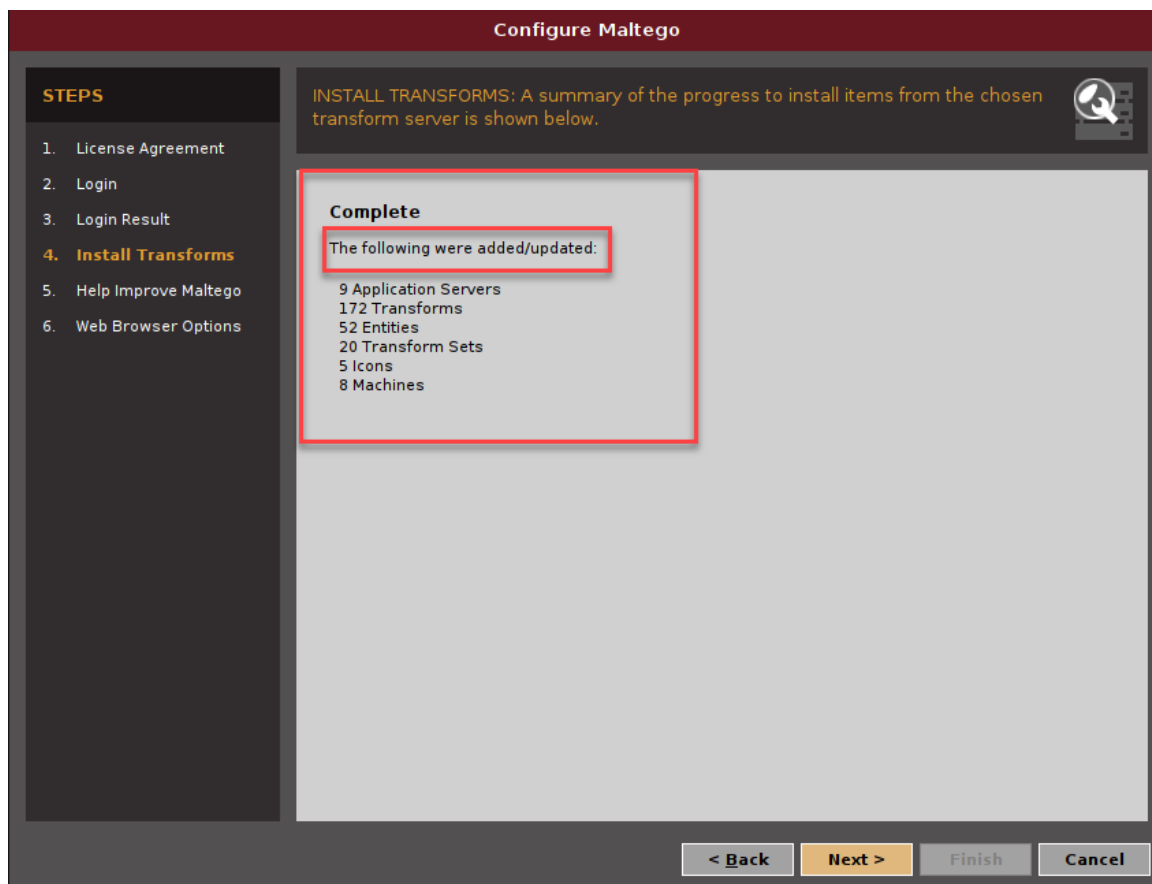
< Back   Next >   Finish   Cancel







## 8. Configuración de Maltego





## 9. Configuración de Maltego



**Configure Maltego**

**STEPS**

1. License Agreement
2. Login
3. Login Result
4. Install Transforms
5. Help Improve Maltego
6. **Web Browser Options**

WEB BROWSER OPTIONS: Select the external browser used to open web links clicked in Maltego.

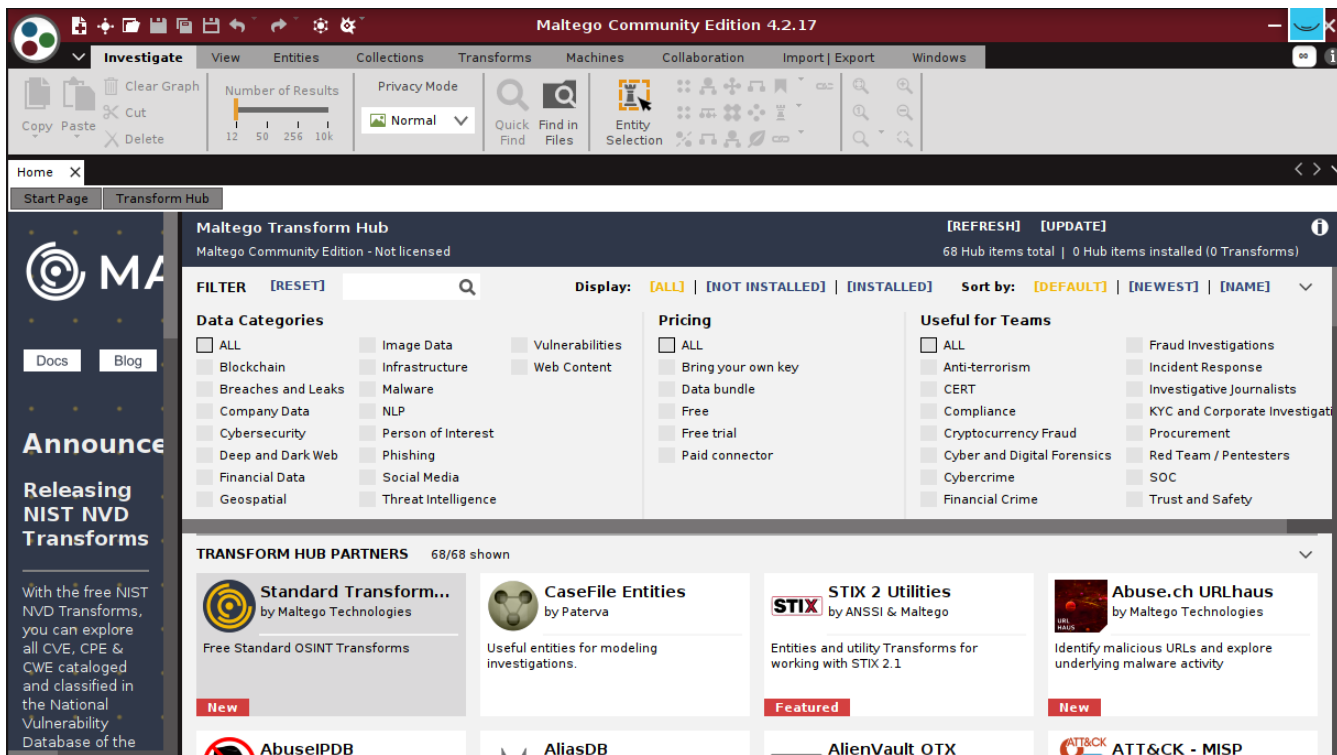
Web Browser: <Default System Browser> **Edit...**

< Back   Next >   **Finish**   Cancel





## 10. Configuración de Maltego



The screenshot displays the Maltego Community Edition 4.2.17 interface. The top menu bar includes options like Investigate, View, Entities, Collections, Transforms, Machines, Collaboration, Import | Export, and Windows. Below the menu is a toolbar with various icons for file operations and search. The main area is titled 'Maltego Transform Hub' and shows a list of transforms categorized by Data Categories, Pricing, and Useful for Teams. The 'Data Categories' section includes options like ALL, Blockchain, Breaches and Leaks, Company Data, Cybersecurity, Deep and Dark Web, Financial Data, Geospatial, Image Data, Infrastructure, Malware, NLP, Person of Interest, Phishing, Social Media, and Threat Intelligence. The 'Pricing' section includes options like ALL, Bring your own key, Data bundle, Free, Free trial, and Paid connector. The 'Useful for Teams' section includes options like ALL, Anti-terrorism, CERT, Compliance, Cryptocurrency Fraud, Cyber and Digital Forensics, Cybercrime, Financial Crime, Fraud Investigations, Incident Response, Investigative Journalists, KYC and Corporate Investigation, Procurement, Red Team / Pentesters, SOC, and Trust and Safety. The bottom section is titled 'TRANSFORM HUB PARTNERS' and lists various partners like Standard Transform..., CaseFile Entities, STIX 2 Utilities, Abuse.ch URLhaus, AbuseIPDB, AliasDB, AlienVault OTX, and ATT&CK - MISP.





## 11. Configuración de Maltego



Maltego Community Edition 4.2.17

1

2

3

Entity Palette

Search:

Recently Used

Domain  
An internet domain

Devices

Device  
A device such as a phone

Events

DateTime  
Contains a date and a time

Groups

Company

Run View

Transforms

Machines

Company S...

Find Wikip...

Footprint L1

Footprint L2

Footprint L3

Footprint X...

New Graph (1)

acistperu.com

Overview

Detail View

Domain  
maltego Domain  
acistperu.com

Property ...

Hub Transform ...

Properties

Type	Domain
Domain Name	acistperu.com
WHOIS Info	
Graph info	
Weight	0
Incoming	0
Outgoing	0
Bookmark	

1 of 1 entity

FOR DEMO USE ONLY





## 12. Configuración de Maltego



Maltego Community Edition 4.2.17

1 Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

2 Domain An internet domain

3 acistperu

4 Run Transforms

- + All Transforms
- + DNS from Domain
- + Domain owner detail
- + Email addresses from Domain
- + Files and Documents from Domain
- + Machines

Required inputs

The following transforms require inputs:

- To Snapshots between Dates [Wayback Machine]

Begin Date - YYYYMMDD	20100101
End Date - YYYYMMDD	20201231

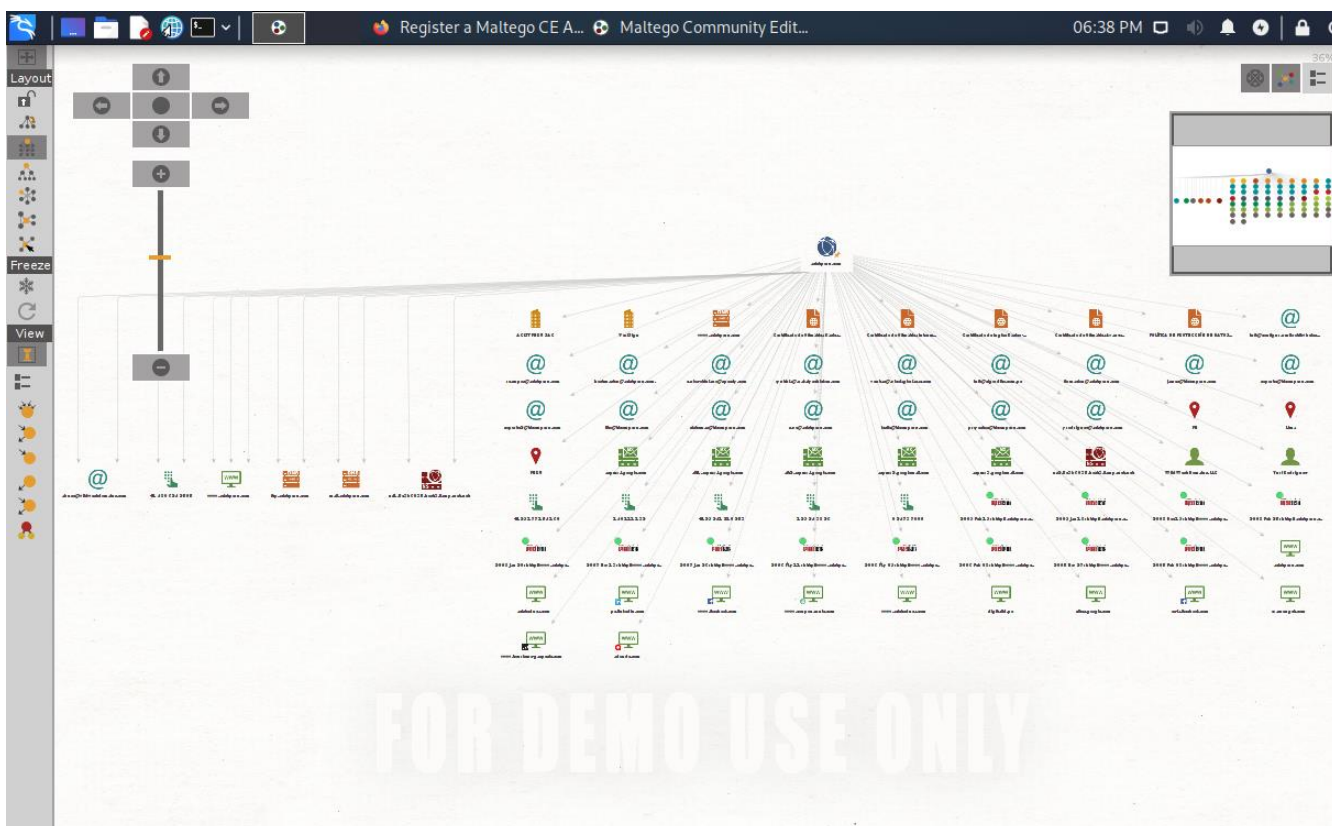
Remember these settings

Run! Cancel





## 13. Configuración de Maltego







# RECONOCIMIENTO DEL OBJETIVO

## ETHICAL HACKING

```
File Actions Edit View Help
Trash

DISCOVER

By Lee Baird

RECON
1. Passive
2. Active
3. Import names into an existing recon-ng workspace
4. Previous menu

Choice: █
```





## 1. Configuración de Discover

<https://github.com/leebaired/discover>

Download, setup and usage

- git clone <https://github.com/leebaired/discover> /opt/discover/
- All scripts must be ran from this location.
- cd /opt/discover/
- ./update.sh

1

2

3

4

RECON

1. Domain
2. Person

SCANNING

3. Generate target list
4. CIDR
5. List
6. IP, range or domain
7. Rerun Nmap scripts and MSF aux

WEB

8. Insecure direct object reference
9. Open multiple tabs in Firefox
10. Nikto
11. SSL







## 2. Configuración de Discover

```
root@kali: /opt
File Actions Edit View Help

(kali@kali)-[~]
$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
(root@kali)-[/home/kali]
# cd /

(root@kali)-[/]
# cd /opt

(root@kali)-[/opt]
# ls
microsoft

(root@kali)-[/opt]
# git clone https://github.com/leebaird/discover /opt/discover/
```





### 3. Configuración de Discover



```
(root@kali)-[/opt]
# ls
discover  microsoft

(root@kali)-[/opt]
# cd discover

(root@kali)-[/opt/discover]
# ls
active.sh      LICENSE      newModules.sh  passive.sh    resource
config         listener.sh  nikto.sh       payload.sh    ssl.sh
directObjectRef.sh  misc        notes          person.sh    update.sh
discover.sh    mods        nse.sh         README.md
domain.sh      msf-aux.sh  parsers        report
generateTargets.sh multiTabs.sh parse.sh       report.sh

(root@kali)-[/opt/discover]
# ./update.sh
```

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NY
Locality Name (eg, city) []:NY
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My own space
Organizational Unit Name (eg, section) []:Tech-tats
Common Name (e.g. server FQDN or YOUR name) []:user1
Email Address []:myownspace@gmail.com
```





## 4. Configuración de Discover



```
Updating locate database.

(root@kali)-[/opt/discover]
# ls
active.sh      LICENSE      newModules.sh  passive.sh    resource
config         listener.sh  nikto.sh       payload.sh    ssl.sh
directObjectRef.sh  misc        notes          person.sh    update.sh
discover.sh    mods        nse.sh        README.md
domain.sh      msf-aux.sh  parsers        report
generateTargets.sh multiTabs.sh parse.sh       report.sh

(root@kali)-[/opt/discover]
# ./discover.sh
```

```
RECON
1. Domain
2. Person

SCANNING
3. Generate 1
4. CIDR
5. List
6. IP, range
7. Rerun Nmap

RECON
1. Passive
2. Active
3. Import name
4. Previous me

Usage
Company: Target
Domain: target.com

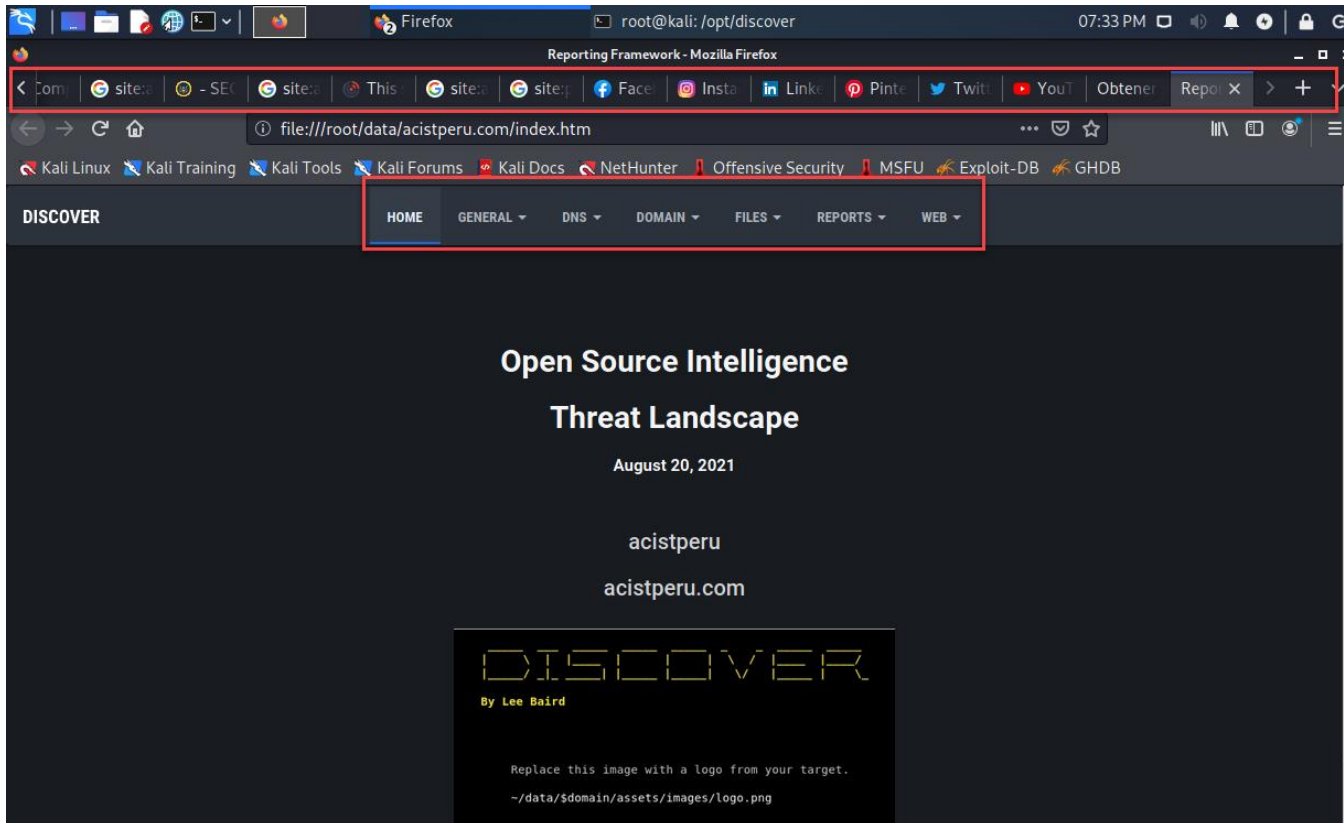
Choice:

Company: acistperu
Domain: acistperu.com
```



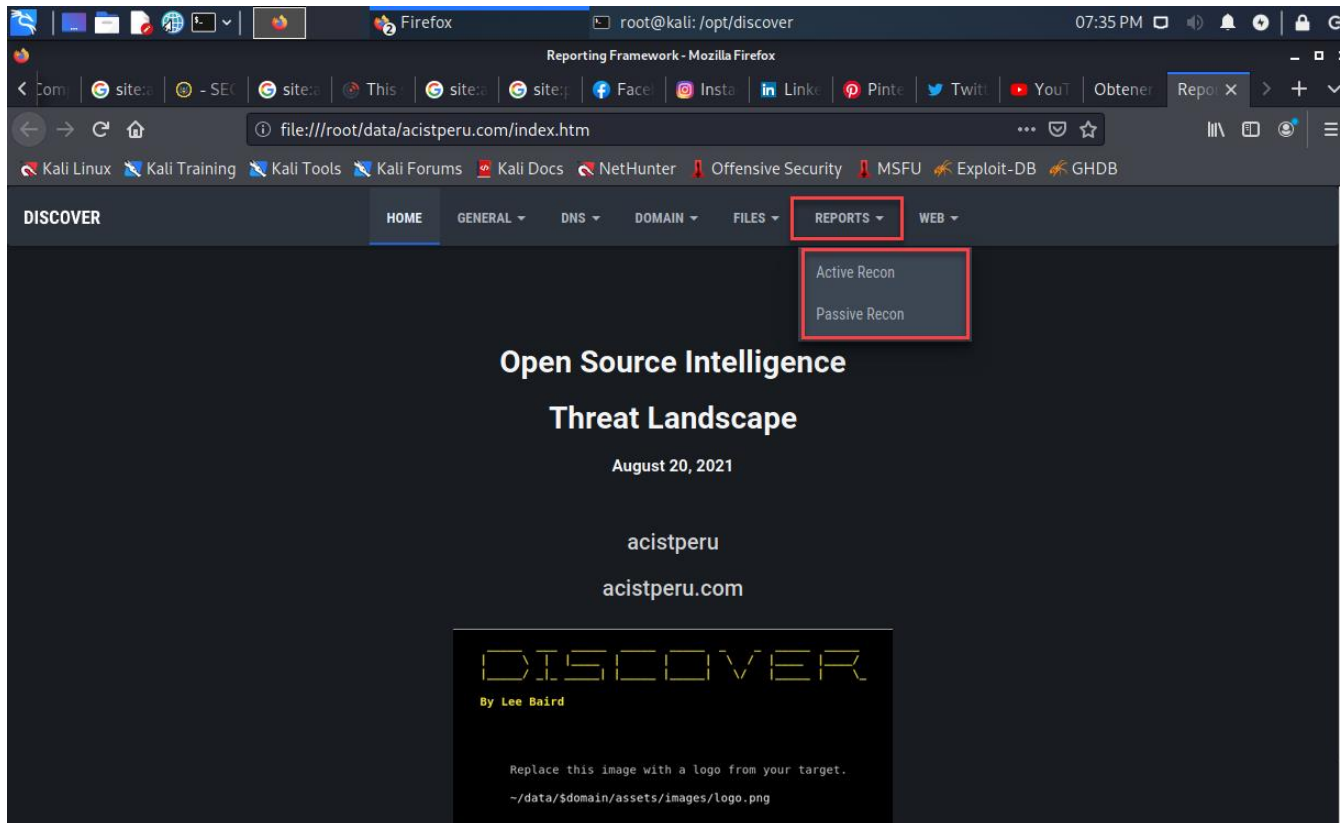


## 5. Configuración de Discover





## 6. Configuración de Discover





## 7. Configuración de Discover



Reports > Passive Recon

### Summary

```
=====
Emails           0
Names            50
DNS Records      15
Hosts            0
Squatting        4
Subdomains       0
```

### Emails (0)

```
=====
```

Reports > Passive Recon

```
-----
A      acistperu.com                67.43.9.110
MX     alt1.aspmx.l.google.com      2a00:1450:400c:c0b::1a
MX     alt1.aspmx.l.google.com      64.233.184.27
MX     alt2.aspmx.l.google.com      142.250.27.27
MX     alt2.aspmx.l.google.com      2a00:1450:4025:401::1b
MX     aspmx2.googlemail.com        2a00:1450:400c:c0b::1b
MX     aspmx2.googlemail.com        64.233.184.27
MX     aspmx3.googlemail.com        142.250.27.27
MX     aspmx3.googlemail.com        2a00:1450:4025:401::1b
MX     aspmx.l.google.com           2800:3f0:4003:c02::1a
MX     aspmx.l.google.com           64.233.186.27
NS     ns1.5e3b6035.host3.llampanet.net 67.43.9.110
NS     ns2.5e3b6035.host3.llampanet.net 67.43.9.110
SOA    ns1.5e3b6035.host3.llampanet.net 67.43.9.110
TXT    _domainkey.acistperu.com v=DKIM1; k=rsa; t=y;
```







## 8. Configuración de Discover



```
Reports > Passive Recon
-----
A      acistperu.com           67.43.9.110
MX     alt1.aspmx.l.google.com 2a00:1450:400c:c0b::1a
MX     alt1.aspmx.l.google.com 64.233.184.27
MX     alt2.aspmx.l.google.com 142.250.27.27
MX     alt2.aspmx.l.google.com 2a00:1450:4025:401::1b
MX     aspmx2.googlemail.com   2a00:1450:400c:c0b::1b
MX     aspmx2.googlemail.com   64.233.184.27
MX     aspmx3.googlemail.com   142.250.27.27
MX     aspmx3.googlemail.com   2a00:1450:4025:401::1b
MX     aspmx.l.google.com      2800:3f0:4003:c02::1a
MX     aspmx.l.google.com      64.233.186.27
NS     ns1.5e3b6035.host3.llampanet.net 67.43.9.110
NS     ns2.5e3b6035.host3.llampanet.net 67.43.9.110
SOA    ns1.5e3b6035.host3.llampanet.net 67.43.9.110
TXT    _domainkey.acistperu.com v=DKIM1; k=rsa; t=y;

Hosts (0)
=====

Squatting (4)
=====
repetition  accistperu.com 178.63.48.152 NS:ns1.mihosting.net      MX:errdomain
subdomain   aci.stperu.com  3.223.115.185 NS:nsg1.namebrightdns.com
subdomain   acist.peru.com    107.0.22.51
subdomain   acistpe.ru.com     141.8.226.34
```





*¡Gracias!* 

