

# DETECCIÓN CON OSINT



ERIC SERRANO MARÍN

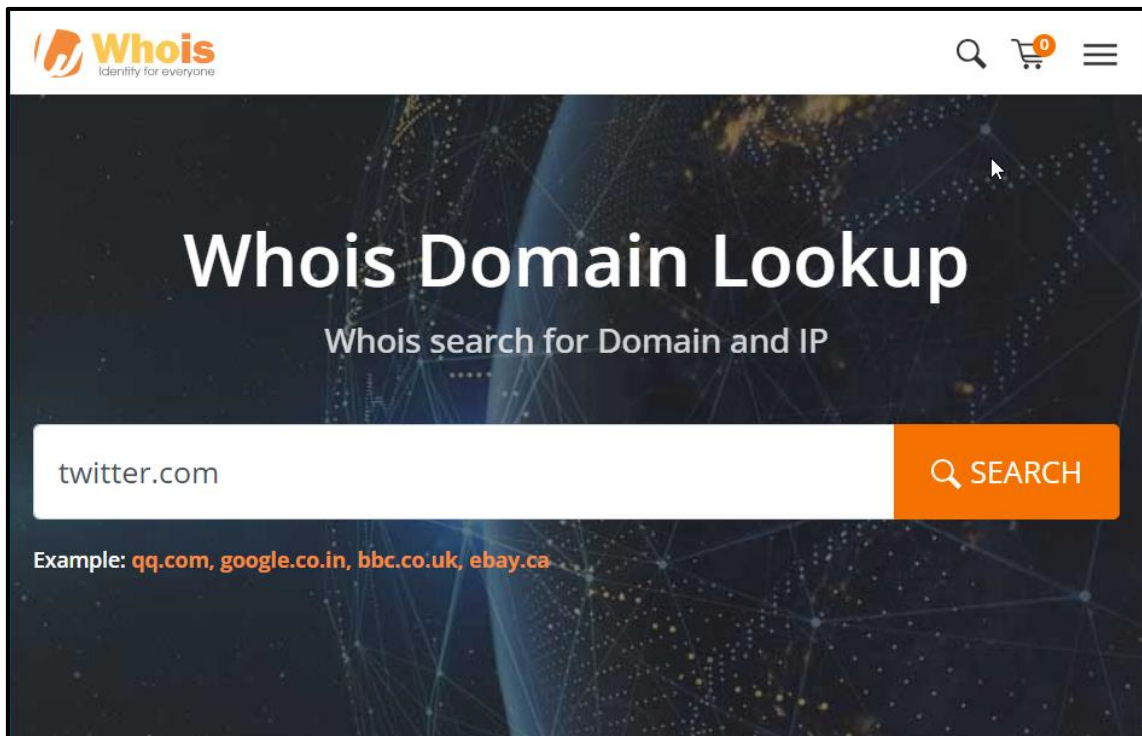
## Contenido

1. Realiza búsquedas OSINT utilizando Whois. ....	3
Información del dominio.....	4
Explicación de datos obtenidos Domain Information .....	4
Información del titular del dominio. ....	5
Explicación de datos obtenidos Registrant Contact.....	5
Información del contacto administrativo.....	6
Explicación de datos obtenidos Administrative Contact.....	6
Información del contacto técnico .....	7
Explicación de datos obtenidos Technical Contact .....	7
¿Has encontrado algo interesante?.....	8
2. Realiza búsquedas OSINT en Archive.org.....	9
3. Utiliza otra herramienta OSINT distinta.....	11
Recon-ng .....	11

## 1. Realiza búsquedas OSINT utilizando Whois.


Consulta la información relativa a algún dominio haciendo uso de una base de datos WhoIS. ¿Has encontrado algo interesante? Explica los datos obtenidos.

Entramos al siguiente enlace: <https://www.whois.com/whois/>



Yo, como podemos observar en la captura voy a buscar información del dominio twitter.com.


Información del dominio

 Domain Information	
Domain:	twitter.com
Registrar:	CSC Corporate Domains, Inc.
Registered On:	2000-01-21
Expires On:	2024-01-21
Updated On:	2023-03-07
Status:	clientTransferProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	a.r06.twtrdns.net a.u06.twtrdns.net b.r06.twtrdns.net b.u06.twtrdns.net c.r06.twtrdns.net c.u06.twtrdns.net d.r06.twtrdns.net d.u06.twtrdns.net

Explicación de datos obtenidos Domain Information

Campo	Descripción	Valor
Domain	Nombre del dominio	twitter.com
Registrar	Entidad que registró el dominio	CSC Corporate Domains, Inc.
Registered On	Fecha de registro del dominio	2000-01-21
Expires On	Fecha de vencimiento del registro	2024-01-21
Updated On	Fecha de la última actualización	2023-03-07
Status	Estado actual del dominio	clientTransferProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Name Servers	Servidores de nombres asociados al dominio	a.r06.twtrdns.net, a.u06.twtrdns.net, b.r06.twtrdns.net, b.u06.twtrdns.net, c.r06.twtrdns.net, c.u06.twtrdns.net, d.r06.twtrdns.net, d.u06.twtrdns.net

Información del titular del dominio.


 **Registrant Contact**

Name:	Twitter, Inc.
Organization:	Twitter, Inc.
Street:	1355 Market Street
City:	San Francisco
State:	CA
Postal Code:	94103
Country:	US
Phone:	+1.4152229670
Fax:	+1.4152220922
Email:	<b>domains</b> @twitter.com

Explicación de datos obtenidos Registrant Contact

Campo	Descripción	Valor
Name	Nombre del titular del dominio	Twitter, Inc.
Organization	Organización del titular del dominio	Twitter, Inc.
Street	Calle de la dirección del titular	1355 Market Street
City	Ciudad de la dirección del titular	San Francisco
State	Estado de la dirección del titular	CA (California)
Postal Code	Código postal de la dirección del titular	94103
Country	País de la dirección del titular	US (Estados Unidos)
Phone	Número de teléfono del titular	+1.4152229670
Fax	Número de fax del titular	+1.4152220922
Email	Correo electrónico del titular	<b>email</b> @twitter.com


## Información del contacto administrativo.

 Administrative Contact	
Name:	Domain Admin
Organization:	Twitter, Inc.
Street:	1355 Market Street
City:	San Francisco
State:	CA
Postal Code:	94103
Country:	US
Phone:	+1.4152229670
Fax:	+1.4152220922
Email:	<a href="mailto:domains@twitter.com">domains@twitter.com</a>

## Explicación de datos obtenidos Administrative Contact

Campo	Descripción	Valor
Name	Nombre del contacto administrativo	Domain Admin
Organization	Organización del contacto administrativo	Twitter, Inc.
Street	Calle de la dirección del contacto administrativo	1355 Market Street
City	Ciudad de la dirección del contacto administrativo	San Francisco
State	Estado de la dirección del contacto administrativo	CA (California)
Postal Code	Código postal de la dirección del contacto administrativo	94103
Country	País de la dirección del contacto administrativo	US (Estados Unidos)
Phone	Número de teléfono del contacto administrativo	+1.4152229670
Fax	Número de fax del contacto administrativo	+1.4152220922
Email	Correo electrónico del contacto administrativo	<a href="mailto:email@twitter.com">email@twitter.com</a>

Información del contacto técnico

 **Technical Contact**

Name:	Tech Admin
Organization:	Twitter, Inc.
Street:	1355 Market Street
City:	San Francisco
State:	CA
Postal Code:	94103
Country:	US
Phone:	+1.4152229670
Fax:	+1.4152220922
Email:	<b>domains-tech</b> @twitter.com

Explicación de datos obtenidos Technical Contact

Campo	Descripción	Valor
Name	Nombre del contacto técnico	Tech Admin
Organization	Organización del contacto técnico	Twitter, Inc.
Street	Calle de la dirección del contacto técnico	1355 Market Street
City	Ciudad de la dirección del contacto técnico	San Francisco
State	Estado de la dirección del contacto técnico	CA (California)
Postal Code	Código postal de la dirección del contacto técnico	94103
Country	País de la dirección del contacto técnico	US (Estados Unidos)
Phone	Número de teléfono del contacto técnico	+1.4152229670
Fax	Número de fax del contacto técnico	+1.4152220922
Email	Correo electrónico del contacto técnico	<b>email</b> @twitter.com

### ¿Has encontrado algo interesante?

Hemos podido encontrar las **medidas de seguridad que tienen activas**, ya que el estado del dominio incluye restricciones como “clientTransferProhibited”, indicando medidas de seguridad activas para prevenir transferencias no autorizadas.

**La Infraestructura de Servidores de Nombres:** Conocer estos detalles puede ser relevante para entender la arquitectura de red de Twitter y potencialmente podría ser explotado si hay vulnerabilidades en estos servidores.



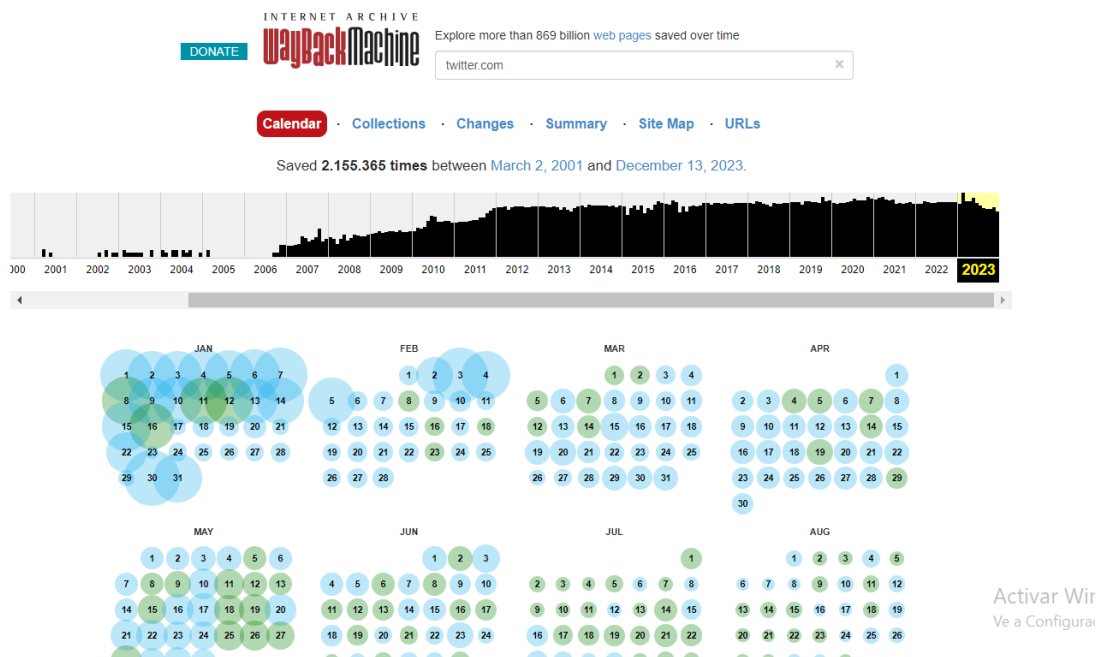
## 2. Realiza búsquedas OSINT en Archive.org.

Busca en archive.org el estado pasado de alguna página que te parezca interesante.

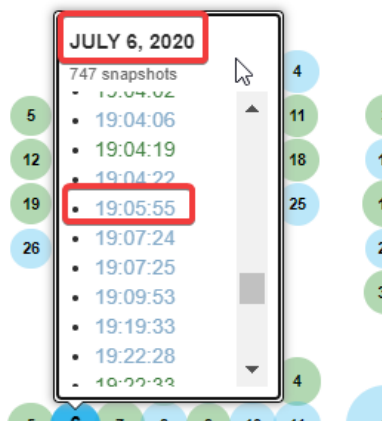
Accederemos al siguiente enlace: <https://archive.org/> y utilizaremos la waybackmachine.



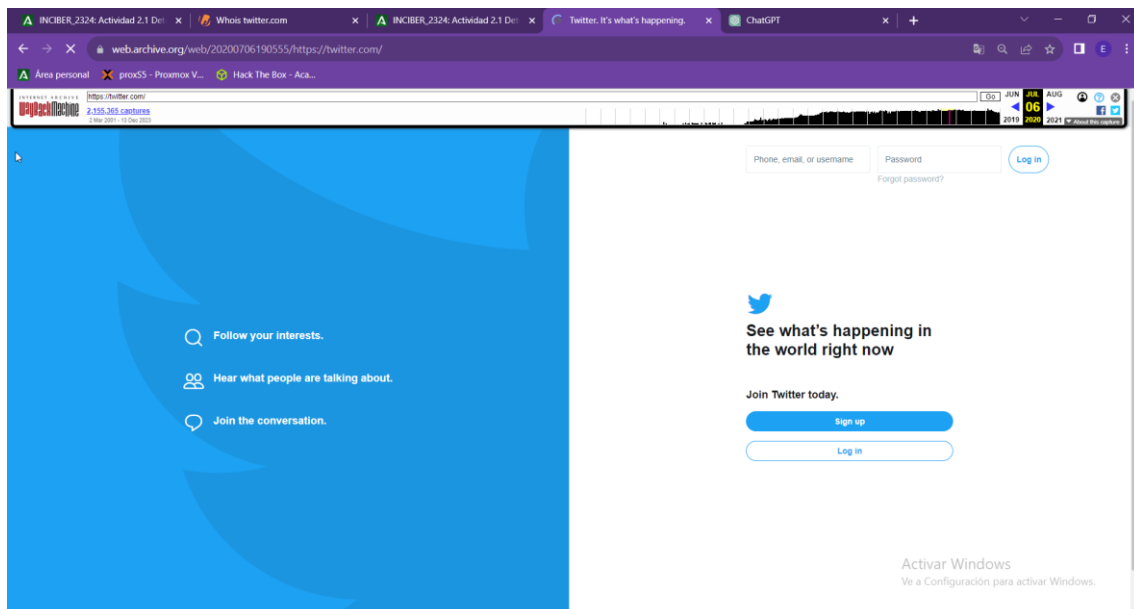
Podemos observar al darle al enter, que podemos ir al estado del dominio de cualquier día y a bastantes horas estos días.



Yo en concreto voy a elegir el 6 de Julio de 2020 a las 19:05:55.



Y ya automáticamente nos lleva al estado de twitter en la fecha que he elegido.



### 3. Utiliza otra herramienta OSINT distinta.

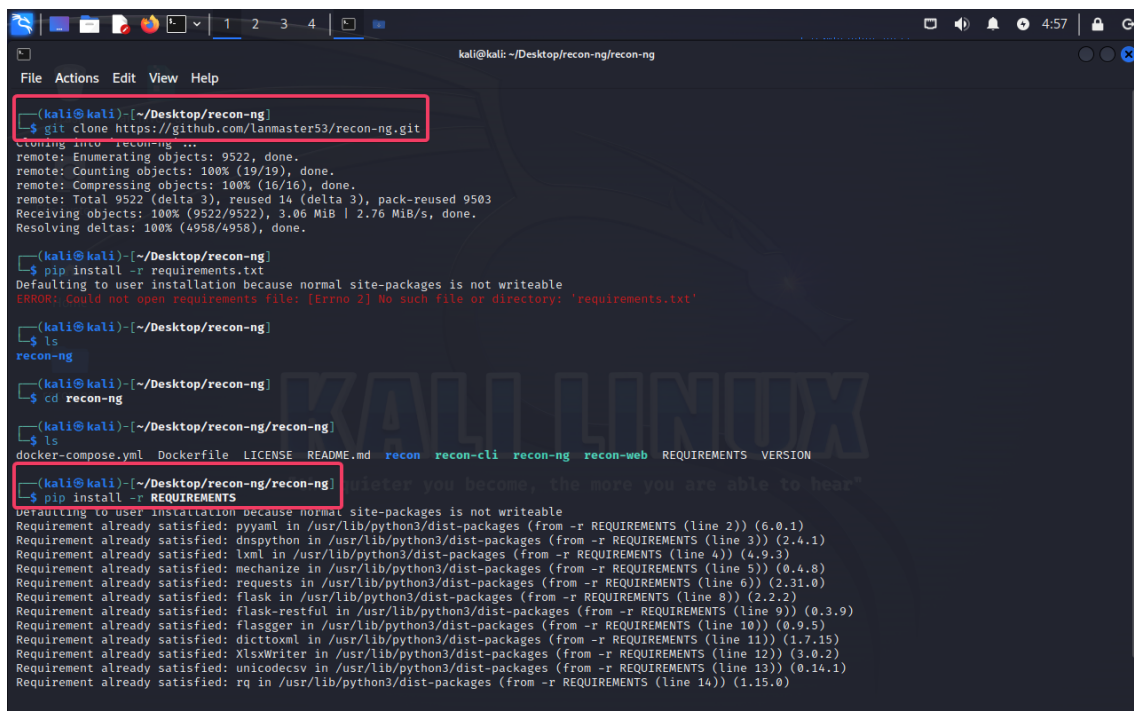
Otra herramienta OSINT que conozcas por tus medios o de otro módulo del curso y que no esté incluida en la unidad.

#### Recon-ng

**git clone** <https://github.com/lanmaster53/recon-ng.git>

**cd recon-ng**

**pip install -r REQUIREMENTS**



```
kali@kali: ~/Desktop/recon-ng/recon-ng
File Actions Edit View Help

(kali@kali)-[~/Desktop/recon-ng]
$ git clone https://github.com/lanmaster53/recon-ng.git
Cloning into 'recon-ng'...
remote: Enumerating objects: 9522, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 9522 (delta 3), reused 14 (delta 3), pack-reused 9503
Receiving objects: 100% (9522/9522), 3.06 MiB | 2.76 MiB/s, done.
Resolving deltas: 100% (4958/4958), done.

(kali@kali)-[~/Desktop/recon-ng]
$ pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
ERROR: Could not open requirements file: [Errno 2] No such file or directory: 'requirements.txt'

(kali@kali)-[~/Desktop/recon-ng]
$ ls
recon-ng

(kali@kali)-[~/Desktop/recon-ng]
$ cd recon-ng

(kali@kali)-[~/Desktop/recon-ng/recon-ng]
$ ls
docker-compose.yml  Dockerfile  LICENSE  README.md  recon  recon-cli  recon-ng  recon-web  REQUIREMENTS  VERSION

(kali@kali)-[~/Desktop/recon-ng/recon-ng]
$ pip install -r REQUIREMENTS
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pyyaml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 2)) (6.0.1)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 3)) (2.4.1)
Requirement already satisfied: lxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 4)) (4.9.3)
Requirement already satisfied: mechanize in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 5)) (0.4.8)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 6)) (2.31.0)
Requirement already satisfied: flask in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 8)) (2.2.2)
Requirement already satisfied: flask-restful in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 9)) (0.3.9)
Requirement already satisfied: flasgger in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 10)) (0.9.5)
Requirement already satisfied: dictxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 11)) (1.7.15)
Requirement already satisfied: XlsxWriter in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 12)) (3.0.2)
Requirement already satisfied: unicodedev in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 13)) (0.14.1)
Requirement already satisfied: rq in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 14)) (1.15.0)
```

Procederemos a iniciar recon-ng.

***./recon-ng***

```

kali@kali: ~/Desktop/recon-ng/recon-ng
File Actions Edit View Help
(kali@kali)~[~/Desktop/recon-ng/recon-ng]
$ ./recon-ng

recon-ng

Sponsored by ...

recon-ng

recon-ng v5.1.2, Tim Tomes (@lanmaster53)

[2] Recon modules
[1] Reporting modules

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

Crearemos un workspace para mantener las cosas ordenadas y que sean fáciles de encontrar.

***workspaces create práctica\_incidentes***

```

[2] Recon modules
[1] Reporting modules

[recon-ng][default] > workspaces create practica_incidentes
[recon-ng][practica_incidentes] > recon-ng -w practica_incidentes
  
```

Ahora buscaremos módulos en Marketplace.

***marketplace search***

```

[recon-ng][practica_incidentes] > marketplace search

+-----+-----+-----+-----+-----+
| Path                                     | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| discovery/info_disclosure/cache_snoop   | 1.1     | not installed | 2020-10-13 |  |  |
| discovery/info_disclosure/interesting_files | 1.2     | not installed | 2021-10-04 |  |  |
| exploitation/injection/command_injector  | 1.0     | not installed | 2019-06-24 |  |  |
| exploitation/injection/xpath_bruter      | 1.2     | not installed | 2019-10-08 |  |  |
| import/csv_file                          | 1.1     | not installed | 2019-08-09 |  |  |
| import/list                              | 1.1     | not installed | 2019-06-24 |  |  |
| import/masscan                           | 1.0     | not installed | 2020-04-07 |  |  |
| import/nmap                              | 1.1     | not installed | 2020-10-06 |  |  |
| recon/companies-contacts/bing_linkedin_cache | 1.0     | not installed | 2019-06-24 |  |  |
| recon/companies-contacts/censys_email_address | 2.0     | not installed | 2021-05-11 | * | * |
| recon/companies-contacts/pen             | 1.1     | not installed | 2019-10-15 |  |  |
| recon/companies-domains/censys_subdomains | 2.0     | not installed | 2021-05-10 | * | * |
| recon/companies-domains/pen             | 1.1     | not installed | 2019-10-15 |  |  |
| recon/companies-domains/viewdns_reverse_whois | 1.1     | not installed | 2021-08-24 |  |  |
| recon/companies-domains/whoxy_dns        | 1.1     | not installed | 2020-06-17 |  |  |
| recon/companies-hosts/censys_org         | 2.0     | not installed | 2021-05-11 | * | * |
  
```

Podemos filtrar por ejemplo por nombre, como en este ejemplo.

### ***marketplace search ssl***

```
K = Requires keys. See info for details.
[recon-ng][practica_incidentes] > marketplace search ssl
[*] Searching module index for 'ssl' ...

+-----+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| recon/domains-hosts/ssl_san | 1.0 | not installed | 2019-06-24 | | |
| recon/hosts-hosts/ssltools | 1.0 | not installed | 2019-06-24 | | |
| recon/ports-hosts/ssl_scan | 1.1 | not installed | 2021-08-24 | | |
+-----+-----+-----+-----+-----+-----+

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

Vamos a instalar un módulo de los que hemos visto anteriormente, concretamente hackertarget.

### ***marketplace install hackertarget***

```
[recon-ng][practica_incidentes] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][practica_incidentes] > █
```

Para empezar a usar el módulo, primero tendremos que cargarlo.

### ***modules load hackertarget***

```
[*] Reloading modules ...
[recon-ng][practica_incidentes] > modules load hackertarget
[recon-ng][practica_incidentes][hackertarget] > █
```

Una vez lo tenemos cargado, como es la primera vez que vamos a usarlo vamos a usar el comando help, para saber el funcionamiento del módulo.

### help

```
[recon-ng][practica_incidentes] > modules load hackertarget
[recon-ng][practica_incidentes][hackertarget] > help

Commands (type [help!?] <topic>):

back           Exits the current context
dashboard      Displays a summary of activity
db             Interfaces with the workspace's database
exit           Exits the framework
goptions       Manages the global context options
help           Displays this menu
info           Shows details about the loaded module
input          Shows inputs based on the source option
keys           Manages third party resource credentials
modules        Interfaces with installed modules
options        Manages the current context options
pdb            Starts a Python Debugger session (dev only)
reload         Reloads the loaded module
run            Runs the loaded module
script         Records and executes command scripts
shell          Executes shell commands
show           Shows various framework items
spool          Spools output to a file
```

Ahora tenemos que darle un source para que pueda hacer las búsquedas.

### options set SOURCE twitter.com

```
[recon-ng][practica_incidentes][hackertarget] > options set SOURCE twitter.com
SOURCE => twitter.com
[recon-ng][practica_incidentes][hackertarget] > █
```

Comprobamos que el source haya cambiado usando info.

### info

```
SOURCE => twitter.com
[recon-ng][practica_incidentes][hackertarget] > info

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    twitter.com      yes       source of input (see 'info' for details)

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

Ahora para ejecutarlo solo tendremos que poner run.

### ***run***

Aquí tenemos el resultado en gif del comando run: <https://i.imgur.com/xksdl5x.gif>

Podemos ver los hosts que nos ha encontrado de forma más clara usando show hosts.

### ***show hosts***

Aquí tenemos el resultado en gif del comando show hosts:

<https://i.imgur.com/DdjToAb.gif>

En alguna captura/gif saldrá también tesla.com, ya que he querido probar también con tesla. Aquí la prueba.

```
[recon-ng][practica_incidentes][hackertarget] > info
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     tesla.com         yes       source of input (see 'info' for details)

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