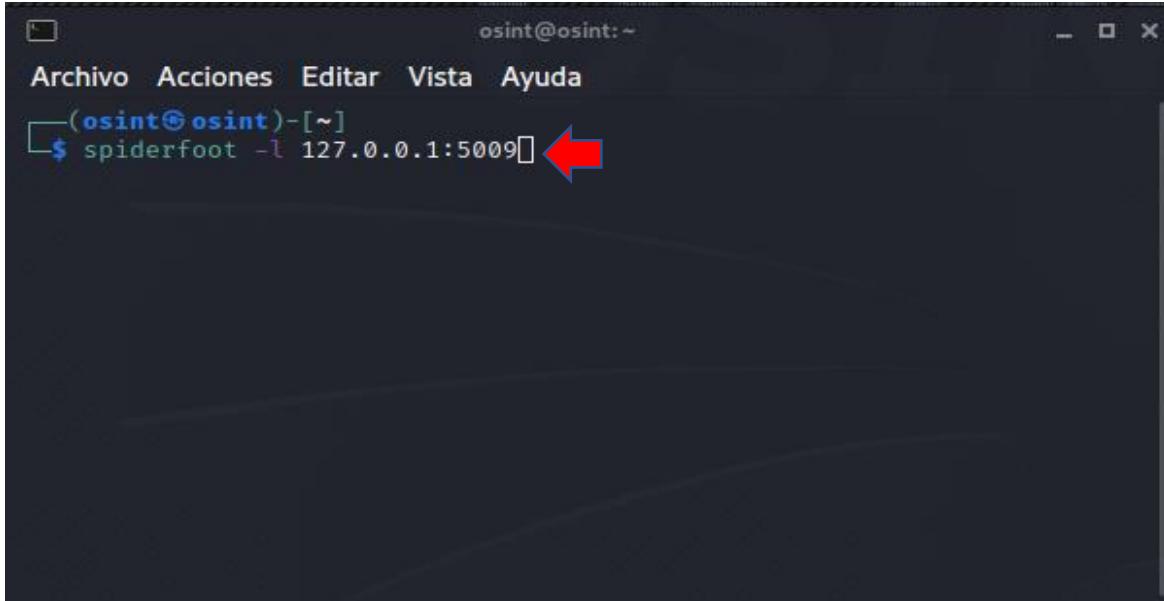


Uso de “Spiderfoot”.

“Spiderfoot” nos ayuda a realizar búsqueda de información sobre: cuentas de correo, nombres de personas, dominios, subdominios, IP y nombres de usuario.

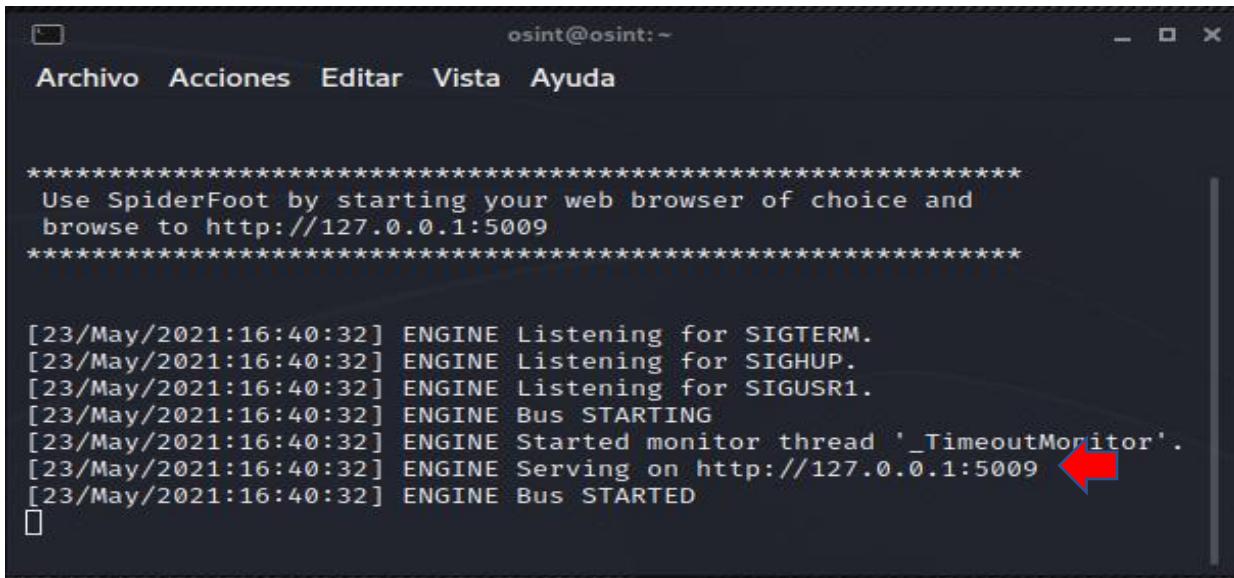
1.-Inicio “`spiderfoot -l 127.0.0.1:5009`”.



```
osint@osint:~  
Archivo Acciones Editar Vista Ayuda  
[(osint@osint) ~] $ spiderfoot -l 127.0.0.1:5009
```

A screenshot of a terminal window titled "osint@osint:~". The menu bar includes "Archivo", "Acciones", "Editar", "Vista", and "Ayuda". The command line shows the user has typed "spiderfoot -l 127.0.0.1:5009". A red arrow points to the command line.

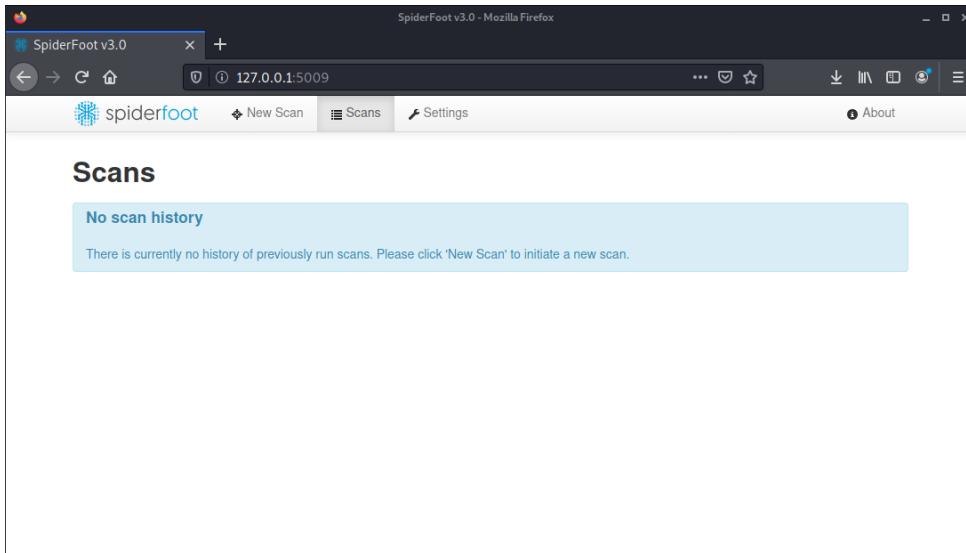
2.-Una vez iniciado nos vamos a la “url” que nos indica “<http://127.0.0.1:5009>” (Sin cerrar la terminal).



```
osint@osint:~  
Archivo Acciones Editar Vista Ayuda  
  
*****  
Use SpiderFoot by starting your web browser of choice and  
browse to http://127.0.0.1:5009  
*****  
  
[23/May/2021:16:40:32] ENGINE Listening for SIGTERM.  
[23/May/2021:16:40:32] ENGINE Listening for SIGHUP.  
[23/May/2021:16:40:32] ENGINE Listening for SIGUSR1.  
[23/May/2021:16:40:32] ENGINE Bus STARTING  
[23/May/2021:16:40:32] ENGINE Started monitor thread '_TimeoutMonitor'.  
[23/May/2021:16:40:32] ENGINE Serving on http://127.0.0.1:5009  
[23/May/2021:16:40:32] ENGINE Bus STARTED
```

A screenshot of a terminal window titled "osint@osint:~". The menu bar includes "Archivo", "Acciones", "Editar", "Vista", and "Ayuda". The terminal displays the logs of the SpiderFoot engine starting up, including messages about listening for SIGTERM, SIGHUP, and SIGUSR1 signals, and starting its own bus. It also indicates it is serving on port 5009. A red arrow points to the line "[23/May/2021:16:40:32] ENGINE Serving on http://127.0.0.1:5009".

3.-Al teclear la “url” indicada en el paso anterior nos dirigirá a la página principal



4.-Para realizar un escaneo nos dirigimos a la pestaña New Scan, en donde colocaremos el nombre del escaneo, y al hacer clic sobre el campo Target, nos indicara los parámetros posibles de búsqueda.

The Seed Target can be one of the following. SpiderFoot will automatically detect the target type based on the format of your input.

Domain Name: e.g. example.com
IPv4 Address: e.g. 1.2.3.4
IPv6 Address: e.g. 2606:4700:4700::1111
Hostname/Sub-domain: e.g. abc.example.com
Subnet: e.g. 1.2.3.0/24
ASN: e.g. 1234
E-mail address: e.g. bob@example.com
Phone Number: e.g. +12345678901 (E.164 format)
Human Name: e.g. "John Smith" (must be in quotes)
Username: e.g. "jsmith2000" (must be in quotes)

All SpiderFoot modules will be used to collect information about the target. A piece of information about the target will be obtained and analysed.

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

piece of information about the target will be obtained and analysed.

net.

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

5.- Una vez que completamos los parámetros dar clic en “Run Scan”, para iniciar el escaneo.

The screenshot shows the 'New Scan' configuration page. It includes fields for 'Scan Name' (set to 'Nombre de la investigación') and 'Seed Target' (set to 'javier@hotmail.com'). Below these are three tabs: 'By Use Case', 'By Required Data', and 'By Module'. Under 'By Use Case', the 'All' option is selected, described as 'Get anything and everything about the target.' A note states: 'All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.' Other options include 'Footprint' (Understand what information this target exposes to the Internet.), 'Investigate' (Best for when you suspect the target to be malicious but need more information.), and 'Passive' (When you don't want the target to even suspect they are being investigated.). A red arrow points to the 'Run Scan' button at the bottom left. A note below it says: 'Note: Scan will be started immediately.'

6.- EL avance del escaneo se puede visualizar en la pestaña Scans, y al finalizar dar “click” en el nombre del escaneo para observar los resultados.

The screenshot shows the 'Scans' results page. It displays a table of completed scans. The first scan in the list is titled 'Nombre de la investigación' and was run against 'javier@hotmail.com'. It started on '2021-07-04 13:58:36' and finished on '2021-07-04 14:01:47'. The status is 'FINISHED' with 156 elements. A red arrow points to the scan name 'Nombre de la investigación'. The top navigation bar includes 'New Scan', 'Scans' (which is selected), and 'Settings'.

Name	Target	Started	Finished	Status	Elements	Action
Nombre de la investigación	javier@hotmail.com	2021-07-04 13:58:36	2021-07-04 14:01:47	FINISHED	156	

7.-Una vez que damos “Click” en el nombre del objetivo, nos dirigirá a la interfaz de los resultados en donde se podrá navegar para el análisis de la información.

The screenshot shows the SpiderFoot v3.0 web application interface. The title bar reads "SpiderFoot v3.0" and the address bar shows "127.0.0.1:5009/scaninfo?id=98C1BAB5". The main header includes the "spiderfoot" logo, "New Scan", "Scans", "Settings", and "About" buttons. Below the header is a section titled "Nombre de la investigación". A navigation bar below this section contains "Status", "Browse", "Graph", "Scan Settings", and "Log" buttons, along with a search bar and download/copy icons. The main content area is a table with the following data:

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	17	17	2021-07-04 14:01:21
Email Address	1	1	2021-07-04 13:58:50
Hacked Email Address	125	125	2021-07-04 14:00:48
Leak Site URL	9	9	2021-07-04 14:01:44
PGP Public Key	1	1	2021-07-04 14:01:32
Raw Data from RIRs/APIs	2	2	2021-07-04 14:00:49
Username	1	1	2021-07-04 14:00:49