

## Práctica de laboratorio: Uso de herramientas OSINT

### Objetivos

En esta práctica de laboratorio, explorará varias herramientas de OSINT que los evaluadores de penetración usan comúnmente.

- Examinar los recursos de OSINT
- Usar SpiderFoot
- Investigar reconocimiento
- Encuentre archivos interesantes con Recon-ng

### Aspectos básicos/Situación

Al realizar actividades de recopilación de información, el reconocimiento pasivo utiliza datos abiertos y de acceso público para guiar los esfuerzos de reconocimiento activo y recopilar información sobre la empresa y los empleados. En OSINT, los datos son de código abierto. Las herramientas OSINT pueden ser de código abierto o no. Algunas herramientas son gratuitas y abiertas, otras requieren registro para usar versiones gratuitas y otras requieren una tarifa para su uso. OSINT comúnmente usa fuentes de datos que están disponibles para cualquier hacker, por lo que parte del esfuerzo de una prueba de penetración es informar sobre información confidencial comúnmente disponible para evaluar las vulnerabilidades que puede causar. Los objetivos de OSINT son:

- Determinar la huella digital de la organización.
- Determinar qué datos sobre la organización están disponibles para los delincuentes ciberneticos.

### Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

### Instrucciones

#### Parte 1: Examinar los recursos de OSINT

##### Paso 1: Acceder al marco de OSINT

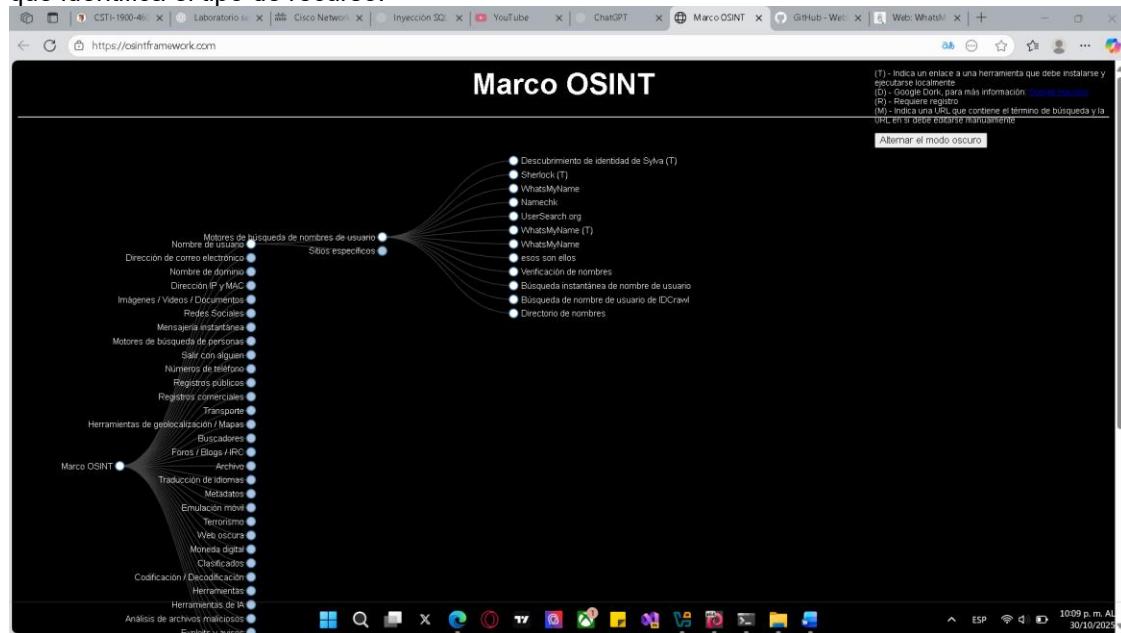
El marco de trabajo de OSINT es una forma útil de visualizar las herramientas y los recursos de OSINT que están disponibles. Desafortunadamente, está un poco desactualizado y algunos recursos ya no están disponibles. Sigue siendo valioso ayudarlo a comprender los tipos de herramientas disponibles y sus usos. En muchos casos, los enlaces siguen siendo buenos.

##### Hacer captura de pantalla de cada punto a continuación

- a. Vaya al sitio del marco de OSINT en <https://osintframework.com/>.
- b. Verá una estructura vertical en forma de árbol que consta de categorías de herramientas y recursos OSINT a los que se puede acceder desde el marco. Haga clic en Nombre de **usuario** en la parte superior del árbol. Luego verá aparecer dos subcategorías. Haga clic en cada uno para abrir los árboles de recursos de cada subcategoría. Nota: en la esquina superior derecha de la página hay una leyenda

## Práctica de laboratorio: Uso de herramientas OSINT

que identifica el tipo de recurso.



- c. En **Username Search Engines**, haga clic en “**WhatsMyName(T)**”.
- d. El enlace lo lleva a un repositorio de Git para el proyecto **WhatsMyName**. En el contenido de **README.md** de la herramienta, se enumeran los diversos sitios que implementan **WhatsMyName**. No dude en explorarlos, pero haremos clic en el primer enlace <https://whatsmyname.app/> para visitar un sitio web gratuito que implementa **WhatsMyName**.

This screenshot shows the GitHub repository page for **WebBreacher / WhatsMyName**. The repository has 2,729 confirmations and 355 contributors. The code tab is selected, showing a list of files and their commit history:

- .github/fluxos de trabajo: Eliminar .github/workflows/check-for-dupe-url.yml (last month)
- Scripts: Refactorizar: Reescribir en Python con clasificación de enca... (5 months ago)
- .gitignore: Actualización de .gitignore (3 years ago)
- CODE\_OF\_CONDUCT.md: Cambios de administrador (last year)
- CONTRIBUTING.md: "Limpieza" general (9 months ago)
- LICENSE.md: "Limpieza" general (9 months ago)
- README.md: Agregar la aplicación NameSeeker a README.md (2 weeks ago)
- SECURITY.md: Actualizar SECURITY.md (3 months ago)
- sample.json: Cambios de administrador (last year)
- whatsmyname.png: Agregar imagen de encabezado a Readme.md (5 years ago)
- wmn-data-schema.json: Cambiar el orden de los encabezados (4 months ago)
- wmn-data.json: (4 months ago)

The repository description states: "Este repositorio tiene el archivo JSON necesario para realizar la enumeración de usuarios en varios sitios web." It includes filters for **ptón**, **Oscuro**, **Usuarios**, **nombre de usuario**, and **socint**. The sidebar shows repository statistics: 10 stars, 2.2k forks, 355 issues, and 76 collaborators.

La organización matriz del sitio, <https://www.osintcombine.com/>, tiene varias herramientas gratuitas interesantes disponibles.

## Práctica de laboratorio: Uso de herramientas OSINT

- e. En el cuadro de búsqueda, escriba algunos nombres de usuario, cada uno en una línea separada. Utilice sus propios nombres de usuario u otros que encuentre. Intente buscar en Internet una lista de palabras de nombres de **usuario comunes** para otros posibles términos de búsqueda. Puede filtrar los resultados según los filtros de categoría, pero, por ahora, solo haga clic en el botón verde de la lupa para iniciar la búsqueda.

En una prueba de penetración, usaría otra herramienta, como **SpiderFoot** (a continuación) para encontrar nombres de usuario en direcciones de correo electrónico que están asociadas con una empresa o dominio.

- f. Investigue los resultados. Puede abrir los enlaces a las cuentas desde los rectángulos verdes o desde la tabla de resultados.
- g. WhatsMyName proporciona un informe muy flexible de los resultados. La tabla de resultados puede ordenarse por columna y puede exportar los resultados como CSV o PDF para generar informes. Además, puede filtrar fácilmente por nombre de usuario y buscar dentro de los resultados. Por último, obtiene enlaces a las páginas de perfil de los usuarios en muchos sitios diferentes.

¿Cuál es el valor de realizar búsquedas de nombres de usuario y enumeración de cuentas?

The screenshot shows a web browser window with the URL <https://whatsmyname.app>. At the top, there's a search bar with the placeholder "Ingrese los nombres de usuario en el cuadro de búsqueda, seleccione cualquier filtro de categoría y haga clic en el icono de búsqueda o presione CTRL+Entrar". Below the search bar, a dropdown menu labeled "Filtros de categoría" is open, showing three options: "alanlozano", "alan.lozano", and "alan\_israel". A green search button with a magnifying glass icon is to the right of the search bar. To the right of the search bar, there's a red button with a circular arrow icon. Below the search area, a message says "Filtro activo: Todos (excluye NSFW)". There are four buttons: "Mostrar encontrados", "Mostrar falsos positivos", "Mostrar no encontrados", and "Mostrar todo". A "Abrir todos los enlaces" button is also present. The main content area displays a grid of 12 cards, each representing a found account. The cards include: "Archivo de nuestro O.", "Blogspot", "Chess.com", "Chess.com", "chatango.com", "Calendy", "Etoro", "Eyeem", "Flipboard", "GitHub", "Genus (Artistas)", and "camino de goma". Each card contains the user name, category, and a link to the account. To the right of the grid, there's a table titled "Filtrar por nombre de usuario:" with three entries: "Alanlozano", "alan.lozano", and "alan\_israel". Below the table, there are buttons for "Mostrar 50 filas", "Copiar", "CSV", and "PDF". A "Buscar:" input field is also present. The table has columns: "NOMBRE", "SITIO", "DE USUARIO", "CATEGORÍA", and "ENLACE". The data in the table is as follows:

| NOMBRE      | SITIO                 | DE USUARIO | CATEGORÍA | ENLACE                                                                                                                                                                                              |
|-------------|-----------------------|------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| alan.lozano | Archivo de nuestro O. | afición    |           | <a href="https://archiveofourown.org/users/alan.lozano">https://archiveofourown.org/users/alan.lozano</a>                                                                                           |
| Alanlozano  | Blogspot              | blog       |           | <a href="http://alanlozano.blogspot.com">http://alanlozano.blogspot.com</a>                                                                                                                         |
| Alanlozano  | Calendy               | Misc       |           | <a href="https://calendly.com/alanlozano">https://calendly.com/alanlozano</a>                                                                                                                       |
| Alanlozano  | chatango.com          | social     |           | <a href="https://alanlozano.chatango.com">https://alanlozano.chatango.com</a>                                                                                                                       |
| alan_israel | Chess.com             | juego      |           | <a href="https://www.chess.com/member/alan_israel">https://www.chess.com/member/alan_israel</a>                                                                                                     |
| Alanlozano  | Chess.com             | juego      |           | <a href="https://www.chess.com/member/alanlozano">https://www.chess.com/member/alanlozano</a>                                                                                                       |
| Alanlozano  | Etoro                 | finanzas   |           | <a href="https://www.etoro.com/people/jue 10:14 p. m. AL (Hora local) jueves, 30 de octubre de 2025">https://www.etoro.com/people/jue 10:14 p. m. AL (Hora local) jueves, 30 de octubre de 2025</a> |
| alan.lozano | Eyeem                 | arte       |           | <a href="https://www.eyeem.com/u/alanlozano">https://www.eyeem.com/u/alanlozano</a>                                                                                                                 |
| alan.lozano | Flipboard             | tech       |           |                                                                                                                                                                                                     |
| alan.lozano | GitHub                |            |           |                                                                                                                                                                                                     |
| alan.lozano | Genus (Artistas)      |            |           |                                                                                                                                                                                                     |
| alan.lozano | camino de goma        |            |           |                                                                                                                                                                                                     |

Identificar cuentas públicas vinculadas a un alias para conocer la huella digital de una persona u organización.

Correlacionar identidades (mismo alias/fotos/bio) para confirmar que varias cuentas pertenecen a la misma entidad.

Detectar reutilización de nombres/creenciales que pueda facilitar ataques de phishing o acceso no autorizado.

Revelar información pública útil para el reconocimiento (contactos, repositorios, datos personales) que guíe pruebas y análisis.

Priorizar vectores de ataque o mitigación: encontrar cuentas con datos sensibles o accesos críticos.

Generar evidencia reproducible (exports CSV/PDF) para documentación y reportes en pruebas autorizadas.

## Parte 2: Usar SpiderFoot

SpiderFoot es un escáner OSINT automatizado. Está incluido con Kali. SpiderFoot consulta más de 1000 fuentes de información abiertas y presenta los resultados en una GUI fácil de usar. SpiderFoot también se puede ejecutar desde una consola. SpiderFoot siembra su escaneo con uno de los siguientes:

- Nombres de dominio
- Direcciones IP
- Dirección de subred
- Número de sistema autónomo (ASN)
- Direcciones de correos electrónicos
- Números de teléfono
- Nombres personales

SpiderFoot ofrece la opción de elegir escaneos según el caso de uso, los datos requeridos y el módulo de SpiderFoot. Los casos de uso son:

- Todo: obtenga toda la información posible sobre el objetivo. Este caso de uso puede tardar mucho en completarse.
- Huella: comprenda el perímetro de la red del objetivo, las identidades asociadas y otra información que se obtiene mediante el rastreo web extenso y el uso de motores de búsqueda.
- Investigar: se trata de objetivos que sospecha que tienen un comportamiento malicioso. Se devolverán las huellas, las búsquedas en listas negras y otras fuentes que informan sobre sitios maliciosos.
- Pasivo: este tipo de escaneo se utiliza si no es deseable que el objetivo sospeche que se está analizando. Esta es una forma de OSINT pasivo.

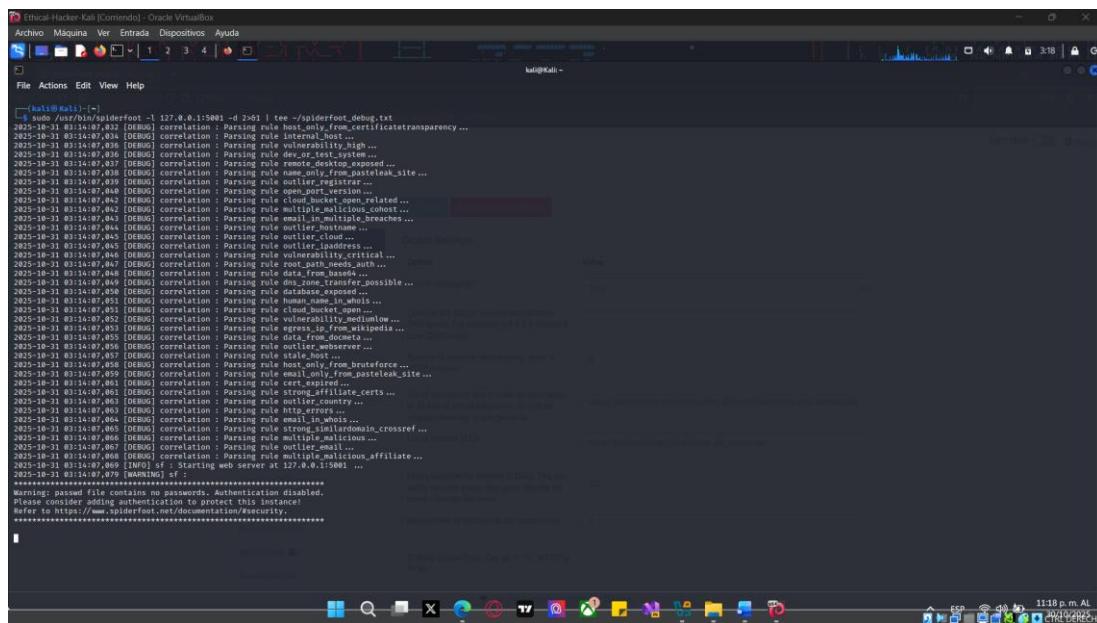
### Paso 1: Inicie y ejecute SpiderFoot.

En una terminal, ingrese el siguiente comando:

```
└── (kali㉿Kali)-[~]
└─$ spiderfoot -l 127.0.0.1:5001
```

El comando debe ejecutarse sin errores. Abra un navegador e ingrese la dirección IP y el puerto para la GUI de SpiderFoot. Verá aparecer la interfaz de SpiderFoot. Si es la primera vez que se abre SpiderFoot en esta VM, verá la pantalla Scans (Escaneos). Esta pantalla muestra una lista de todos los escaneos ejecutados recientemente. En este ejemplo, está vacío.

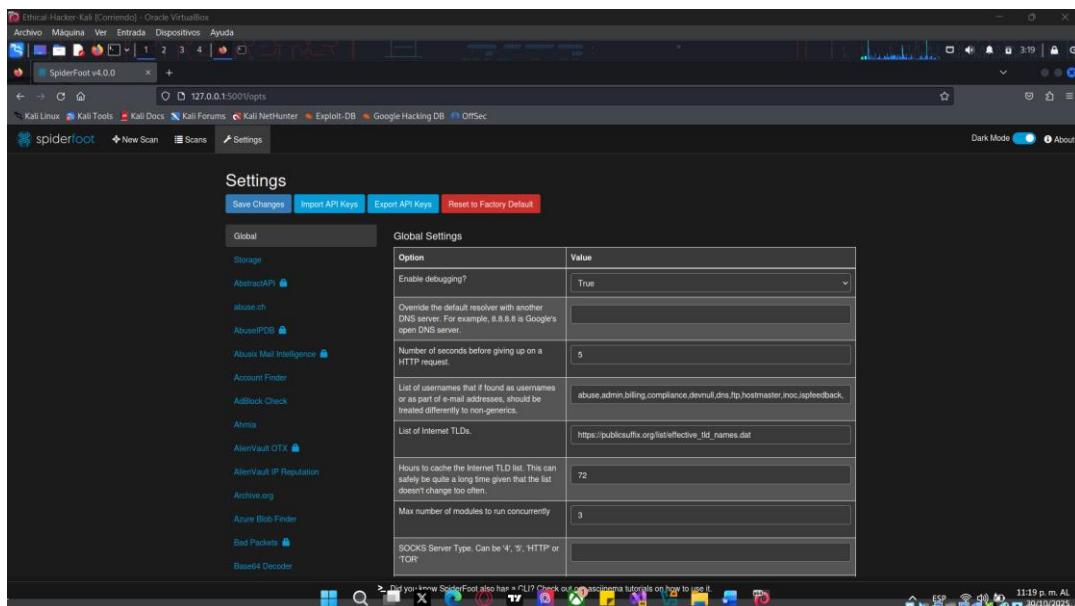
## Práctica de laboratorio: Uso de herramientas OSINT



A terminal window titled "kali@Kali: ~" showing the output of a SpiderFoot analysis command. The command was run with the following parameters: -l 127.0.0.1:5000 -d 2>&1 | tee ->spiderfoot\_debug.txt. The output shows numerous log entries from 2023-10-31 at 00:14:07.032 to 2023-10-31 at 03:14:07.079, detailing various correlation rules being parsed and executed. The logs include entries for "correlation : Parsing rule host\_only\_from\_certificate\_transparency ...", "correlation : Parsing rule internal\_host ...", "correlation : Parsing rule dev\_or\_test\_ip ...", "correlation : Parsing rule remote\_desktop\_exposed ...", "correlation : Parsing rule multiple\_leak\_site ...", "correlation : Parsing rule outlier\_register ...", "correlation : Parsing rule open\_port\_version ...", "correlation : Parsing rule multiple\_vulnerabilities ...", "correlation : Parsing rule multiple\_malicious\_hosts ...", "correlation : Parsing rule email\_in\_multiple\_breaches ...", "correlation : Parsing rule http\_in\_multiple\_breaches ...", "correlation : Parsing rule outlier\_cloud ...", "correlation : Parsing rule outlier\_ipaddress ...", "correlation : Parsing rule root\_path\_needs\_auth ...", "correlation : Parsing rule data\_from\_needs\_auth ...", "correlation : Parsing rule transfer\_possible ...", "correlation : Parsing rule database\_exposed ...", "correlation : Parsing rule http\_in\_multiple\_breaches ...", "correlation : Parsing rule cloud\_bucket ...", "correlation : Parsing rule vulnability\_medium\_low ...", "correlation : Parsing rule multiple\_vulnerabilities ...", "correlation : Parsing rule data\_from\_documents ...", "correlation : Parsing rule outlier\_webserver ...", "correlation : Parsing rule host\_only\_from\_bruteforce ...", "correlation : Parsing rule email\_only\_from\_pasteleak\_site ...", "correlation : Parsing rule strong\_affiliate\_certs ...", "correlation : Parsing rule outlier\_country ...", "correlation : Parsing rule email\_in\_whois ...", "correlation : Parsing rule strong\_similardomain\_crossref ...", "correlation : Parsing rule outlier\_email ...", "correlation : Parsing rule multiple\_malicious\_affiliate ...", "correlation : Parsing rule http\_in\_multiple\_breaches ...". A warning message at the bottom states: "Warning: passwd file contains no passwords. Authentication disabled. Please consider adding authentication to protect this instance! Refer to https://www.spiderfoot.net/documentation/#security." The terminal window is part of a Kali Linux desktop environment.

### Paso 2: Explore SpiderFoot.

- Antes de comenzar, observe los escáneres que utiliza SpiderFoot para crear sus informes. Vaya a la pestaña **Settings** (Configuración).



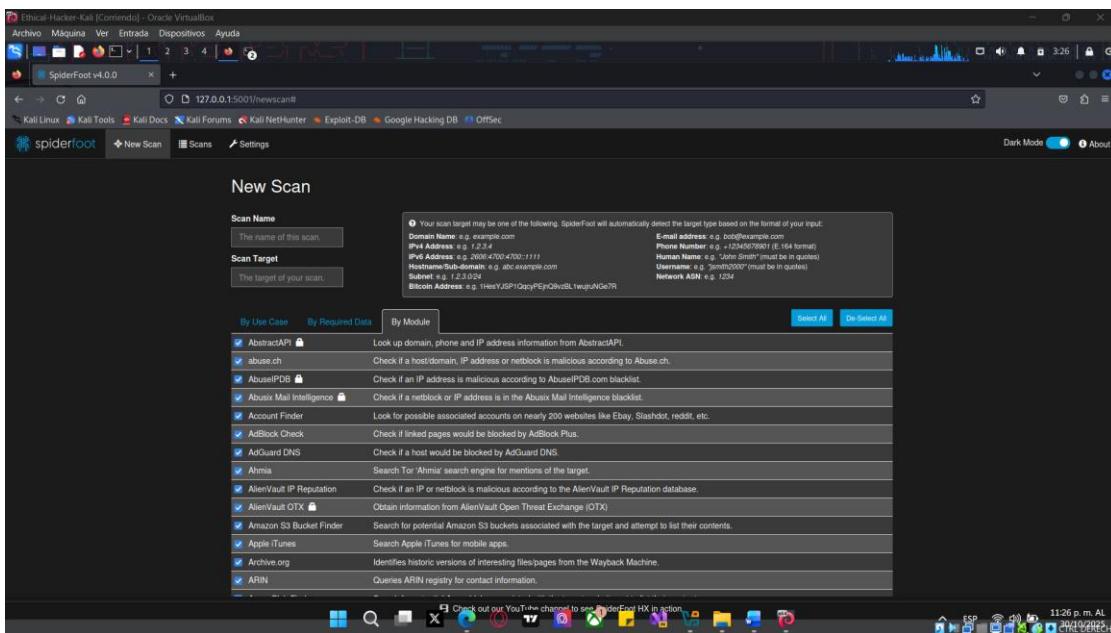
The screenshot shows the "Settings" page of SpiderFoot v4.0. The main interface has tabs for "New Scan", "Scans", and "Settings". The "Settings" tab is active. At the top, there are buttons for "Save Changes", "Import API Keys", "Export API Keys", and "Reset to Factory Default". Below this is a "Global" section with a table of global settings:

| Option                                                                                                                     | Value                                                                      |
|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Enable debugging?                                                                                                          | True                                                                       |
| Override the default resolver with another DNS server. For example, 8.8.8.8 is Google's open DNS server.                   |                                                                            |
| Number of seconds before giving up on a HTTP request.                                                                      | 5                                                                          |
| List of usernames that if found as usernames or as part of e-mail addresses, should be treated differently to non-generic. | abuse.admin.billing.compliance.devnull.dns.tpt.hostmaster.nov.ispfeedback, |
| List of Internet TLDs.                                                                                                     | https://publicsuffix.org/list/effective_tld_names.dat                      |
| Hours to cache the Internet TLD list. This can safely be quite a long time given that the list doesn't change too often.   | 72                                                                         |
| Max number of modules to run concurrently                                                                                  | 3                                                                          |
| SOCKS Server Type. Can be '4', '5', HTTP or TOR                                                                            |                                                                            |

- Las dos primeras entradas del menú de la izquierda están relacionadas con el funcionamiento de SpiderFoot. Las entradas debajo de esto son para los escáneres que usa SpiderFoot. Hay más de 200. Haga clic en los escáneres para ver el nombre del módulo de SpiderFoot, los detalles sobre el escáner y las configuraciones que se pueden realizar, si corresponde. Complete la siguiente tabla con algunos ejemplos. El nombre del escáner está en el menú de configuración. El nombre del módulo aparece en los detalles del escáner. Todos los módulos de SpiderFoot se denominan sfp\_[nombre del módulo].

**Sugerencia:** los escáneres con un candado al lado indican que se necesita una clave de API. Se proporciona más información sobre los requisitos clave en los detalles del escáner. Haga clic en "?" junto a la opción Configuración de API.

## Práctica de laboratorio: Uso de herramientas OSINT



**Sugerencia:** también puede interactuar con SpiderFoot desde el terminal. Puede mostrar todos los módulos que están disponibles en SpiderFoot y canalizar la salida a un archivo de texto. Introduzca **spiderfoot -h** para ver las opciones de la línea de comandos.

```
(kali㉿kali)-[~] $ sudo spiderfoot -h
usage: sf.py [-h] [-d] [-l IP:port] [-m mod1,mod2,...] [-c scanID] [-s TARGET] [-t type1,type2,...] [-u [all,footprint,investigate,passive]] [-T] [-o {tab,csv,json}] [-H] [-n] [-r] [-S LENGTH] [-D DELIMITER] [-f]
                  [-F type1,type2,...] [-x] [-v] [-max-threads MAX_THREADS]

SpiderFoot 4.0.0: Open Source Intelligence Automation.

options:
-h, --help            show this help message and exit
--version           Show version information
-l IP:port          IP and port to listen on.
-m mod1,mod2,...    Modules to enable.
-n                List available modules.
-c scanID, --correlate scanID
                  Take the provided correlation rules against a scan ID.
-s TARGET           Target for the scan (can be a domain or IP).
-t type1,type2,...  Event types to collect (modules selected automatically).
-u [all,footprint,investigate,passive]
                  Select modules automatically by use case
-T                 List available event types.
--types             List available event types.
--tab,csv,json     Don't print field headers, just data.
-H                 Strip newlines from data.
-n                 Don't print field headers, just data.
-r                 Include raw source data in tab/csv output.
-S LENGTH          Maximum data length to display. By default, all data is shown.
-D DELIMITER        Delimiter to use for CSV output. Default is a comma.
-f type1,type2,...  Filter out event types that weren't specified with -t.
-F type1,type2,...  Show only a set of event types separated by commas.
-x                STRICT MODE. Will only enable modules that can directly consume your target, and if -t was specified only those events will be consumed by modules. This overrides -t and -m options.
-v                Display the version and exit.
--version           Display the version and exit.
--max-threads MAX_THREADS
                  Max number of modules to run concurrently.

(kali㉿kali)-[~]
```

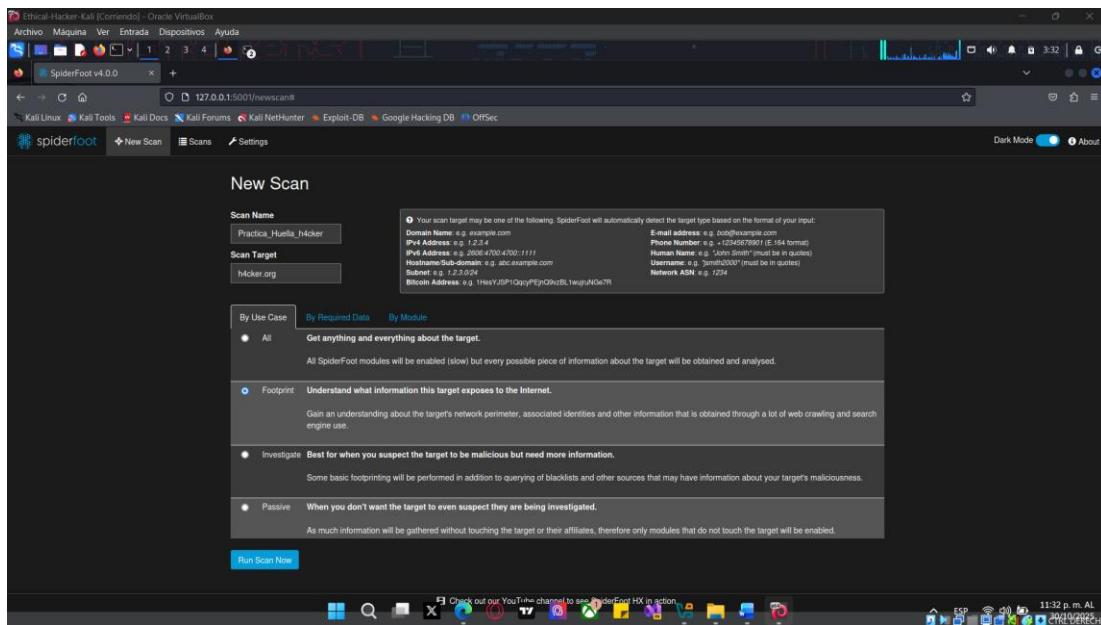
### Paso 3: Ejecute un análisis de SpiderFoot para un dominio.

- Haga clic en la pestaña **New Scan** (Nuevo análisis) en la GUI.
- Introduzca un nombre para el análisis y seleccione un objetivo. En este caso, usaremos **h4cker.org**.
- Escaneará por caso de uso. Tenga en cuenta que también puede escanear por el tipo de información requerida o seleccionando los módulos de escáner individuales que le gustaría utilizar. Al ejecutar escaneos más específicos, puede obtener más información sobre los módulos y la información que se puede recopilar.

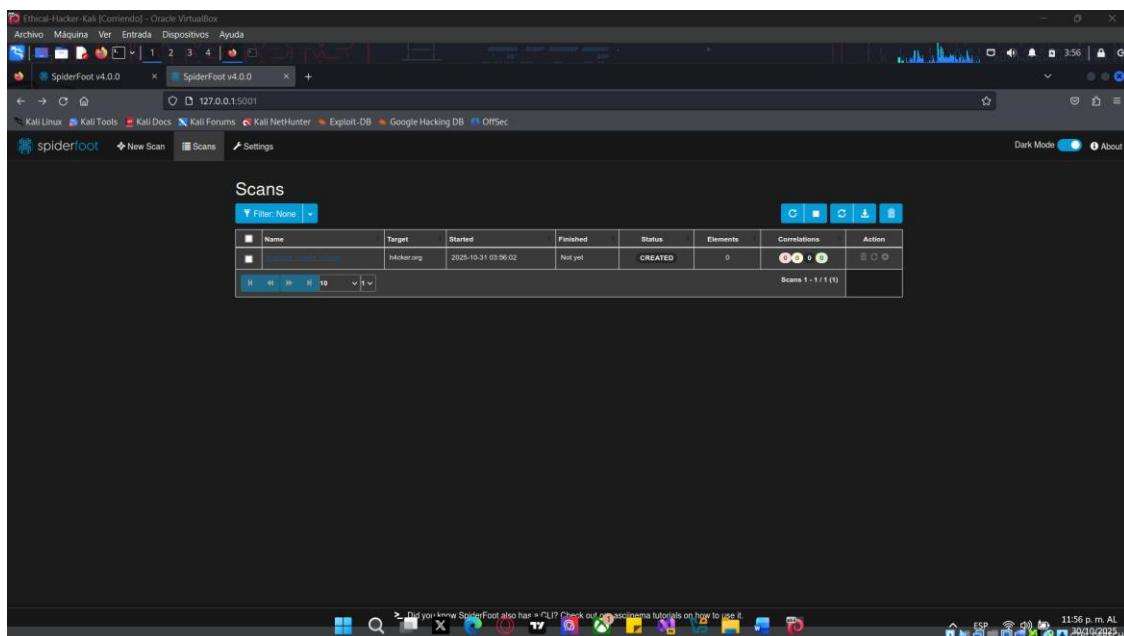
## Práctica de laboratorio: Uso de herramientas OSINT

- d. Seleccione el caso de uso de escaneo como **Huella**.

**Nota:** El análisis de casos de uso de All (Todos) puede utilizar el análisis activo. A menos que tenga permiso para escanear el objetivo, debe evitar esta configuración. Para ser completamente seguro, el caso de uso pasivo debe evitar cualquier problema con el escaneo no autorizado.

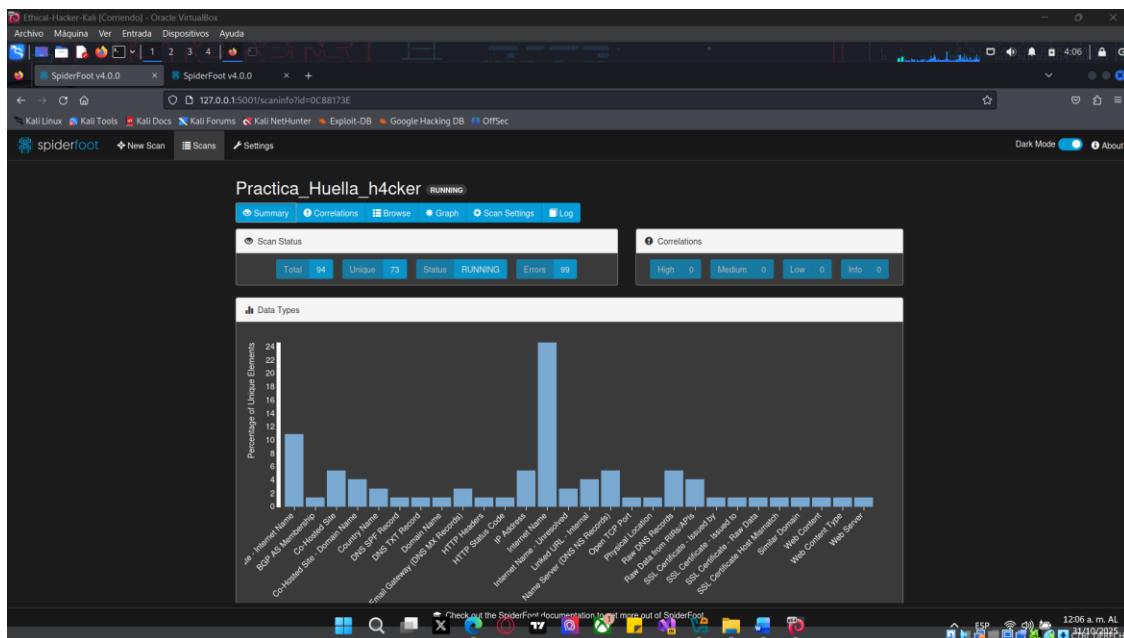


- e. Haga clic en el botón **Ejecutar análisis ahora**.
- f. Debería ver aparecer un gráfico de barras. Las estadísticas de escaneo comenzarán a incrementarse y aparecerán nuevas barras en el gráfico a medida que se obtengan nuevos resultados. Pase el mouse sobre las barras para ver un resumen de los resultados de ese tipo de datos.
- g. Los escaneos de SpiderFoot son muy detallados y pueden llevar mucho tiempo. Dé a este escaneo al menos 30 minutos para que haya una buena recopilación de información. Para obtener la mayor cantidad de detalles, un escaneo puede llevar horas. Mientras se ejecuta el escaneo, puede examinar los resultados.



### Paso 4: Investigue los resultados del escaneo.

- Regrese a los resultados del análisis haciendo clic en la pestaña **Scans**. Verá una tabla con el escaneo que se está ejecutando actualmente y los escaneos anteriores.
- Haga clic en el cuadrado negro en la columna más a la derecha de la tabla de escaneo para detener el escaneo. Parte de la información no está disponible hasta que se cancela o se completa el escaneo.
- Haga clic en el nombre del escaneo en la tabla para volver a la vista del escaneo. Se lo dirigirá a la pestaña **Browse**. Cada fila de la tabla representa los datos encontrados por los distintos módulos. Algunos módulos contribuyen a varios tipos de datos.
- Investigue los resultados.



### Parte 3: Investigar reconocimiento

Recon-ng es un marco OSINT similar al marco de explotación de Metasploit o al Tooklit de ingeniería social (SET). Consta de una serie de módulos que pueden ejecutarse en sus propios espacios de trabajo. Los módulos se pueden configurar para ejecutarse con ajustes de opciones que son específicos del módulo. Esto simplifica la ejecución de Recon-ng en la línea de comandos porque las opciones para los módulos se establecen de forma independiente dentro del espacio de trabajo. Cuando ejecuta el módulo, utiliza esta configuración para realizar sus búsquedas.

Como su nombre lo indica, Recon-ng se usa para realizar una amplia gama de actividades de reconocimiento en diferentes configuraciones que usted proporcione. Algunos módulos están disponibles con la instalación de Kali y otros están disponibles para su descarga e instalación en el mercado de módulos de Recon-ng.

### Paso 1: Crea un espacio de trabajo.

El reconocimiento tiene autocompletado. Presione el botón de tabulación para completar los comandos y las opciones de comando. Utilice la tecla de tabulación dos veces para enumerar los comandos y las opciones disponibles en diferentes lugares de la línea de comandos. Esto resulta bastante útil.

- Para ejecutar Recon-ng, abra una nueva ventana de terminal e ingrese **recon-ng**. También puede iniciar el programa yendo al menú de herramientas de Kali, buscando la aplicación y haciendo clic en el ícono.
- Tenga en cuenta que el indicador del terminal cambia para indicar que está trabajando dentro del marco de reconocimiento. Ingrese **help** para tener una idea de los comandos que están disponibles.

## Práctica de laboratorio: Uso de herramientas OSINT

- c. Recon-ng utiliza espacios de trabajo para aislar las investigaciones entre sí. Los espacios de trabajo se pueden crear para diferentes partes de una prueba o para diferentes clientes, por ejemplo. Escriba **workspaces Help** para ver las opciones del comando workspaces.

```
[recon-ng]# workspaces list
[recon-ng]# workspaces <create|list|load|remove> [...]
[recon-ng]# workspaces Help
Manages workspaces
Usage: workspaces <create|list|load|remove> [...]
```

¿Cómo puede mostrar los espacios de trabajo disponibles?

Ingrese el comando **workspaces list**.

```
[recon-ng]# workspaces list
[recon-ng]# workspaces <create|list|load|remove> [...]
[recon-ng]# workspaces Help
Manages workspaces
Usage: workspaces <create|list|load|remove> [...]
```

¿Cómo se puede eliminar un espacio de trabajo?

## Práctica de laboratorio: Uso de herramientas OSINT

```
[recon-ng v5.1.2, Tim Tones (@lannisters53)]
```

```
[*] No modules enabled/installied.
```

```
[recon-ng][default] > # crear y listar workspaces
```

```
[recon-ng][default] > workspaces create practica
```

```
[recon-ng][practica] > workspaces list
```

| Workspaces | Modified            |
|------------|---------------------|
| default    | 2025-10-31 04:09:22 |
| practica   | 2025-10-31 04:10:26 |

```
[recon-ng][practica] > workspaces select practica
```

```
Manages workspaces
```

```
Usage: workspaces <create|list|load|remove> [ ... ]
```

```
[recon-ng][practica] > workspaces Help
```

```
Manages workspaces
```

```
Usage: workspaces <create|list|load|remove> [ ... ]
```

```
[recon-ng][practica] > workspaces list
```

| Workspaces | Modified            |
|------------|---------------------|
| default    | 2025-10-31 04:09:22 |
| practica   | 2025-10-31 04:10:26 |

```
[recon-ng][practica] > workspaces remove practica
```

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

Ingrese el comando **workspaces remove [nombre\_espacio\_trabajo]**.

- Cree un espacio de trabajo denominado **prueba** ingresando **workspaces create** seguido del nombre del espacio de trabajo. Tenga en cuenta que la solicitud ha cambiado para indicar que se encuentra en este espacio de trabajo.
- Escriba **help** para ver los comandos que están disponibles en los espacios de trabajo.

¿Qué comando saldrá del espacio de trabajo y regresará al indicador principal de Recon-NG?

```
[recon-ng v5.1.2, Tim Tones (@lannisters53)]
```

```
[*] No modules enabled/installied.
```

```
[recon-ng][default] > workspace create prueba
```

```
[recon-ng][default] > workspace create practica
```

```
[recon-ng][practica] > workspaces list
```

| Workspaces | Modified            |
|------------|---------------------|
| default    | 2025-10-31 04:09:22 |
| practica   | 2025-10-31 04:10:55 |

```
[recon-ng][practica] > workspace select practica
```

```
Manages workspaces
```

```
Usage: workspaces <create|list|load|remove> [ ... ]
```

```
[recon-ng][practica] > modules search
```

```
Searches installed modules
```

```
Usage: modules search <regex>
```

```
[recon-ng][practica] > help
```

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

|             |                                          |
|-------------|------------------------------------------|
| back        | Exits the current context                |
| dashboard   | Shows the activity                       |
| db          | Interfaces with the workspace's database |
| exit        | Exits the framework                      |
| help        | Shows help                               |
| index       | Creates a module index (dev only)        |
| keys        | Manages third party resource credentials |
| marketplace | Manages the marketplace                  |
| modules     | Interfaces with installed modules        |
| options     | Manages the current context options      |
| path        | Lists the current path (dev only)        |
| script      | Records and executes command scripts     |
| shell       | Executes shell commands                  |
| show        | Show internal framework items            |
| snapshots   | Manages workspace snapshots              |
| spool       | Spoils output to a file                  |
| workspaces  | Manages workspaces                       |

```
[recon-ng][practica] > back
```

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

### Paso 2: Investigue los módulos.

Recon-NG es un marco modular. Los módulos son programas de Python con diferentes funciones. Se almacenan en un mercado externo que permite a los desarrolladores crear sus propios módulos y aportarlos para que los usen otros.

Regrese a la solicitud de reconocimiento. Introduzca el comando de **modules search**. Esto mostrará los módulos instalados actualmente.

¿Cuántos módulos hay disponibles actualmente?

[Initial Hacking Rail (Contento) - Oracle VirtualBox]

Archivo Máquina Ver Entradas Dispositivos Ayuda

Shell No. 1

File Actions Edit View Help

(+) No modules enabled/installable.

```
[recon-ng][default] > workspace create prueba
[recon-ng][prueba] > workspace create practica
[recon-ng][practica] > workspaces list
```

| Workspaces | Modified            |
|------------|---------------------|
| default    | 2025-10-31 06:09:32 |
| practica   | 2025-10-31 06:19:55 |

```
[recon-ng][practica] > workspaces select practica
Manages workspaces

Usage: workspaces <createlist>[load|remove] [ ... ]
```

```
[recon-ng][practica] > modules search
[+] No modules found.
Searches installed modules

Usage: modules search <regex>
```

```
[recon-ng][practica] > help
Commands (type [help]) <topic>)
```

| Command     | Description                                 |
|-------------|---------------------------------------------|
| back        | Exits the current context                   |
| dashboard   | Displays summary of activity                |
| db          | Interfaces with the workspace's database    |
| exit        | Exits the framework                         |
| help        | Displays help                               |
| index       | Creates a module index (dev only)           |
| modules     | Manages third party repositories            |
| marketplace | Interfaces with the module marketplace      |
| modules     | Interfaces with installed modules           |
| options     | Manages configuration                       |
| pdf         | Starts a Python Debugger session (dev only) |
| script      | Records and executes command scripts        |
| showall     | Shows various framework items               |
| show        | Manages workspace snapshots                 |
| snapshots   | Saves workspace state to file               |
| workspaces  | Manages workspaces                          |

```
[recon-ng][practica] > modules search
[recon-ng][practica] > help
[recon-ng][practica] > search installed modules
[recon-ng][practica] > modules search <regex>
[recon-ng][practica] > 
```

## No hay módulos instalados.

### **Paso 3: Instale un módulo nuevo.**

Recon-ning accede a los módulos del repositorio de Github y los descarga en Kali cuando se instalan.

- a. Busque en los módulos del mercado con **bing** como término de búsqueda. Busque un módulo que no requiera dependencias ni claves de API.

## ¿Qué módulo encontró?

```
[Initial-Hacker-Kit [Console] - Oracle VirtualBox]
Archivo Máquina Ver Entrada Dispositivos Ayuda
Shell No.1
File Actions Edit View Help
K = Requires keys. See Info for details.

[recon-mg][default] > marketplace install recon/domains-hosts/hackertarget
[recon-mg][default] > Marketplace command these: [recon_githubupdate()]
[recon-mg][default] > marketplace Max version exceeded with url: [/marketplace/recon-domains-hosts/modules/recon/domains-hosts/hackertarget.py] (Caused By NewConnectionError('curl/7.51.0 connection to https://github.com/rapid7/recon-githubupdate/recon-domains-hosts/hackertarget.py failed')).

[recon-mg][default] > marketplace install recon/domains-hosts/bing_domain_web
[recon-mg][default] > Marketplace command these: [recon_githubupdate()]
[recon-mg][default] > marketplace Max version exceeded with url: [/marketplace/recon-githubupdate/recon-domains-hosts/bing_domain_web.py] (Caused By NewConnectionError('curl/7.51.0 connection to https://github.com/rapid7/recon-githubupdate/recon-domains-hosts/bing_domain_web.py failed')).

[recon-mg][default] > modules search hackertarget
[recon-mg][default] > Searching installed modules for 'hackertarget' ...

Searches installed modules

Usage: modules search [regex*]

[recon-mg][default] > modules search bing_domain_web
[recon-mg][default] > Searching installed modules for 'bing_domain_web' ...

Searches installed modules

Usage: modules search [regex*]

[recon-mg][default] > Marketplace install recon/domains-hosts/hackertarget
[recon-mg][default] > Marketplace command these: [recon_githubupdate()]
[recon-mg][default] > Reloading modules ...
[recon-mg][default] > Marketplace install recon/domains-hosts/bing_domain_web
[recon-mg][default] > Marketplace command these: [recon_githubupdate()]
[recon-mg][default] > Reloading modules ...
[recon-mg][default] > modules search interesting_files
[recon-mg][default] > Module installed: discovery/info_disclosure/interesting_files
[recon-mg][default] > Reloading modules ...
[recon-mg][default] > modules search hackertarget
[recon-mg][default] > Searching installed modules for 'hackertarget' ...

Recon
[recon-mg][default] > recon/domains-hosts/hackertarget

[recon-mg][default] > modules search bing_domain_web
[recon-mg][default] > Searching installed modules for 'bing_domain_web' ...

Recon
[recon-mg][default] > recon/domains-hosts/bing_domain_web

[recon-mg][default] > Modules search interesting_files
[recon-mg][default] > Searching installed modules for 'interesting_files' ...

Discovery
[recon-mg][default] > discovery/info_disclosure/interesting_files

[recon-mg][default] >
```

recon/domains-hosts/bing domain web

- b. Vea la información de este módulo.
  - c. Para instalar el módulo, copie el nombre completo, incluida la ruta, en el portapapeles.
  - d. Ingrese el comando de **marketplace install** seguido del nombre completo del módulo.

```
[recon-ng] [default] > marketplace install recon/domains-hosts/bing_domain_web
```

- e. Después de la instalación, ingrese el comando de **modules search** para verificar que el nuevo módulo ya esté disponible.

The screenshot shows a terminal window titled 'Ethical Hacker Lab [Comando] - Oracle VirtualBox'. The terminal displays the following session:

```
Shell No. 1
File Actions Edit View Help
Usage: modules search [<regex>]
[recon-ng][default] > modules search bing_domain_web
[*] Searching installed modules for 'bing_domain_web' ...
Searches installed modules
Usage: modules search [<regex>]
[recon-ng][default] > marketplace install recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules...
[recon-ng][default] > marketplace install discovery/info_disclosure/interesting_files
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Reloading modules...
[recon-ng][default] > modules search hackertarget
[*] Searching installed modules for 'hackertarget' ...
Recon
  recon/domains-hosts/hackertarget
[recon-ng][default] > modules search bing_domain_web
[*] Searching installed modules for 'bing_domain_web' ...
Recon
  recon/domains-hosts/bing_domain_web
[recon-ng][default] > modules search interesting_files
[*] Searching installed modules for 'interesting_files' ...
Discovery
  discovery/info_disclosure/interesting_files
[recon-ng][default] > marketplace install recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Reloading modules...
[recon-ng][default] > modules search
Discovery
  discovery/info_disclosure/interesting_files
Recon
  recon/domains-hosts/bing_domain_web
  recon/domains-hosts/hackertarget
[recon-ng][default] >
```

- f. Repita el proceso para instalar el módulo **hackertarget**.

### Paso 4: Ejecute los nuevos módulos.

- Crea un nuevo espacio de trabajo. Nómbralo como desee.
- Para comenzar a trabajar con un módulo, debe inicializarse. Ingrese **modules load hackertarget** para comenzar a trabajar con el módulo. Tenga en cuenta que el mensaje cambia para reflejar el módulo cargado.
- Cada módulo tiene su propio entorno. Los desarrolladores de recon-ng se han encargado de mantener la coherencia del marco, por lo que los mismos comandos están disponibles para cada módulo. Sin embargo, las opciones pueden variar. Escriba **info** en el indicador del módulo para ver detalles importantes sobre el módulo.

Práctica de laboratorio: Uso de herramientas OSINT

- d. En lugar de pasar opciones en la línea de comandos, en Recon-**ng** establece las opciones y luego ingresa un comando simple para ejecutar el módulo. Utilice el comando **options set source** para establecer la única opción para este módulo. Complete el comando especificando el objetivo como **hackxor.net**.
  - e. Verifique la configuración de la opción con el comando **info**.
  - f. Escriba **run** para ejecutar el módulo.
  - g. Inspeccione la salida del comando. La salida se almacena en una base de datos para que pueda consultarla más adelante. Los datos almacenados son específicos del lugar de trabajo en el que se recopilaron.

A screenshot of the RECON-NET application window titled "ethical-hacker-Kali [Concurrent - Oracle VirtualBox]". The window displays network reconnaissance results for several hosts. At the top, there's a menu bar with "File", "Actions", "Edit", "View", "Entrada", "Dispositivos", and "Ayuda". Below the menu is a toolbar with icons for file operations like Open, Save, Print, and Help. The main content area shows a table of network information for each host. The columns include "Country", "Name", "Host", "Ip Address", "Latitude", "Longitude", "Notes", and "Region". A large watermark of the word "RECON-NET" is overlaid across the center of the screen.

- h. Ingrese el comando **dashboard**. Esto consulta la base de datos de Recon-**ng** y proporciona un resumen de la información que se ha recopilado. Es específico de este espacio de trabajo.
    - i. El comando **show** muestra los datos de categorías específicas. Ingrese el comando **show hosts** para mostrar la lista de hosts detectados.

## Práctica de laboratorio: Uso de herramientas OSINT

Ethical-Hacker-Kali [Comiendo] - Oracle VirtualBox

File Actions Edit View Help

SUMMARY

[+] 7 total (7 new) hosts found.

[recon-ng][laboratorio][hackertarget] > dashboard

Activity Summary

Module | Runs

recon/domains-hosts/hackertarget | 1

Results Summary

Category | Quantity

Domains | 0  
Companies | 0  
Netblocks | 0  
Locations | 0  
Vulnerabilities | 0  
Ports | 0  
Hosts | 7  
Contacts | 0  
Credentials | 0  
Leaks | 0  
Pushpins | 0  
Profiles | 0  
Repositories | 0

[recon-ng][laboratorio][hackertarget] > show hosts

| rowid | host                       | ip.address     | region | country | latitude | longitude | notes | module       |
|-------|----------------------------|----------------|--------|---------|----------|-----------|-------|--------------|
| 1     | Host: research.hackxor.net | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 2     | dreaded.hackxor.net        | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 3     | hkrb.hackxor.net           | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 4     | hmc.hackxor.net            | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 5     | intranet.hackxor.net       | 16.66.18.18    |        |         |          |           |       | hackertarget |
| 6     | research1.hackxor.net      | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 7     | transparency.hackxor.net   | 138.66.117.124 |        |         |          |           |       | hackertarget |

[+] 7 rows returned

[recon-ng][laboratorio][hackertarget] >

Ethical-Hacker-Kali [Comiendo] - Oracle VirtualBox

File Actions Edit View Help

SOURCE => hackxor.net

[recon-ng][laboratorio][bing\_domain\_web] > run

HACKXOR.NET

[+] URL: https://www.bing.com/search?first=0&q=domain%3Ahackxor.net

[recon-ng][laboratorio][bing\_domain\_web] > show hosts

| rowid | host                       | ip_address     | region | country | latitude | longitude | notes | module       |
|-------|----------------------------|----------------|--------|---------|----------|-----------|-------|--------------|
| 1     | Host: research.hackxor.net | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 2     | hmc.hackxor.net            | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 3     | hkrb.hackxor.net           | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 4     | hmc.hackxor.net            | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 5     | intranet.hackxor.net       | 16.66.18.18    |        |         |          |           |       | hackertarget |
| 6     | research.hackxor.net       | 138.66.117.124 |        |         |          |           |       | hackertarget |
| 7     | transparency.hackxor.net   | 138.66.117.124 |        |         |          |           |       | hackertarget |

[+] 7 rows returned

[recon-ng][laboratorio][bing\_domain\_web] > dashboard

Activity Summary

Module | Runs

recon/domains-hosts/bing\_domain\_web | 1

recon/domains-hosts/hackertarget | 1

Results Summary

Category | Quantity

Domains | 0  
Companies | 0  
Netblocks | 0  
Locations | 0  
Vulnerabilities | 0  
Ports | 0  
Hosts | 7  
Contacts | 0  
Credentials | 0  
Leaks | 0  
Pushpins | 0  
Profiles | 0  
Repositories | 0

[recon-ng][laboratorio][bing\_domain\_web] >

- j. Ahora repita el proceso con el módulo de **bing**. Compare los resultados con el módulo **hackertarget**.

¿Cuántos subdominios encontró el módulo? ¿Cómo se compara esto con el módulo **hackertarget**?

El módulo **bing\_domain\_web** encontró 7 subdominios, exactamente la misma cantidad que el módulo **hackertarget**. Ambos módulos detectaron los mismos hosts asociados al dominio **hackxor.net**, lo que demuestra que sus fuentes (Hackertarget API y Bing Search) ofrecieron resultados equivalentes para este objetivo.

### Paso 5: Investigue la interfaz web.

Recon-ng tiene una interfaz web que simplifica y mejora la visualización de los resultados almacenados en las bases de datos de Recon-ng. También permite una fácil exportación de las tablas de resultados con fines de generación de informes.

- a. Abra una nueva terminal.

Práctica de laboratorio: Uso de herramientas OSINT

- b. Ingrese el comando **recon-web** para iniciar el proceso de Recon-ng Server. Tenga en cuenta el resultado del comando.
  - c. En una nueva pestaña del navegador, acceda a la página web con la información de URL proporcionada en el resultado.
  - d. La interfaz web muestra datos del espacio de trabajo predeterminado cuando se abre por primera vez. Haga clic en el nombre del espacio de trabajo naranja en la parte superior de la página para mostrar datos de diferentes espacios de trabajo.

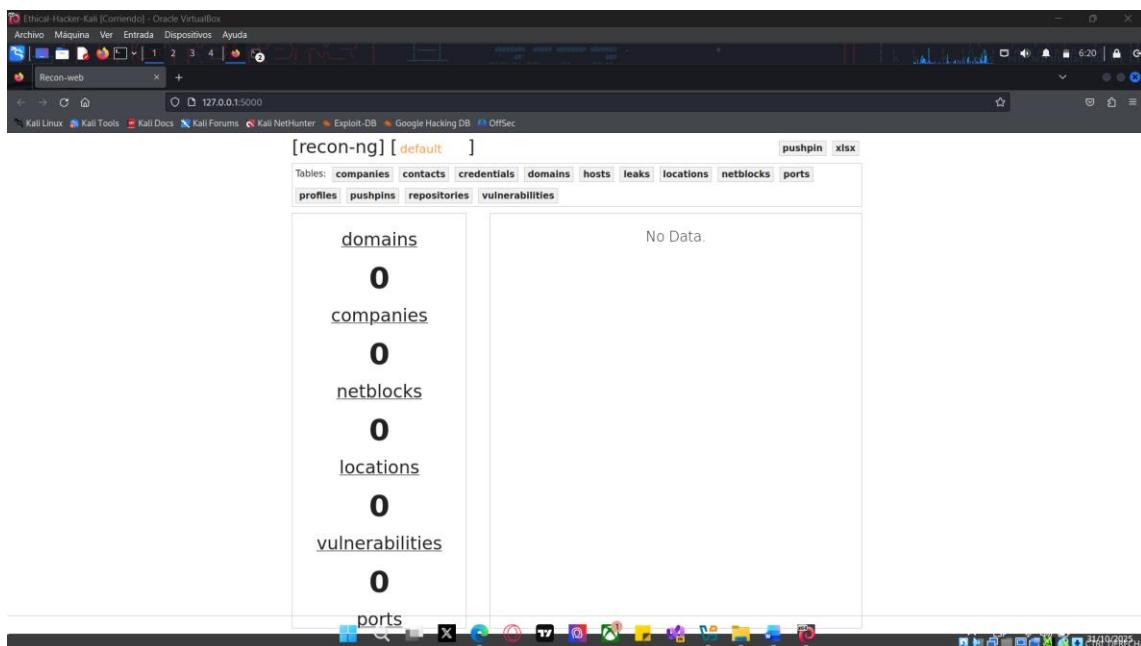
ethical-hacker-Kali [Comiendo] - Oracle VirtualBox

File Actions Edit View Help

[x] recon-web

-----  
\* Welcome to Recon-MDB, the analytics and reporting engine for Recon-ng!  
\* This is the web interface for Recon-MDB. The URL must begin with 'http://'.  
\* Recon-web includes the Recon-API, which can be accessed via the '/api/' URL.  
-----  
\* Marketplace disabled.  
\* Version check disabled.  
\* Workspace initialized: default  
-----  
\* No workspaces found. Please create one or import from a file.  
\* No reports found. Please run a scan or import from a file.  
\* No domains found. Please run a scan or import from a file.  
\* No netblocks found. Please run a scan or import from a file.  
\* No locations found. Please run a scan or import from a file.  
\* No vulnerabilities found. Please run a scan or import from a file.  
-----  
\* Running on http://127.0.0.1:5000  
Press CTRL-C to quit

127.0.0.1 - - [31/Oct/2025 06:19:23] "GET / HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /skelton.css HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /fontawesome.css HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /jquery.min.js HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /sortable.js HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /recon.js HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /recon.ng HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /favicon.ico HTTP/1.1" 404 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /api/recon HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /api/cables/ HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /api/dashboard/ HTTP/1.1" 200 -  
127.0.0.1 - - [31/Oct/2025 06:19:24] "GET /api/reports/ HTTP/1.1" 200 -



#### **Parte 4: Encuentre archivos interesantes con Recon-ng**

En esta parte de la práctica de laboratorio, instalaremos y utilizaremos otro complemento.

## Paso 1: Instale otro módulo.

- Busque en el mercado un módulo que descubra archivos interesantes en un dominio. El complemento que use no debe tener dependencias ni requisitos clave.

¿Qué módulo encontró?

```
[recon-ng][laboratorio] > bing_domain_web
[recon-ng][laboratorio] > recon/domains-hosts/bing_domain_web
[recon-ng][laboratorio] > 7 rows returned
[recon-ng][laboratorio] > dashboard
[recon-ng][laboratorio] > Activity Summary
[recon-ng][laboratorio] > domains 0
[recon-ng][laboratorio] > companies 0
[recon-ng][laboratorio] > netblocks 0
[recon-ng][laboratorio] > locations 0
[recon-ng][laboratorio] > Results Summary
[recon-ng][laboratorio] > Category | Quantity
[recon-ng][laboratorio] > Domains | 0
[recon-ng][laboratorio] > Companies | 0
[recon-ng][laboratorio] > Netblocks | 0
[recon-ng][laboratorio] > Locations | 0
[recon-ng][laboratorio] > Vulnerabilities | 0
[recon-ng][laboratorio] > Hosts | 0
[recon-ng][laboratorio] > Contacts | 0
[recon-ng][laboratorio] > Credentials | 0
[recon-ng][laboratorio] > Users | 0
[recon-ng][laboratorio] > Plugins | 0
[recon-ng][laboratorio] > Profiles | 0
[recon-ng][laboratorio] > Repositories | 0
[recon-ng][laboratorio] > [recon-ng][laboratorio] > discovery/info_disclosure/interesting_files
[recon-ng][laboratorio] > Modules installed: discovery/info_disclosure/interesting_files
[recon-ng][laboratorio] > Reloading modules...
[recon-ng][laboratorio] > modules search interesting_files
[recon-ng][laboratorio] > Searching installed modules for 'interesting_files'...
[recon-ng][laboratorio] > Discovery
[recon-ng][laboratorio] > discovery/info_disclosure/interesting_files
[recon-ng][laboratorio] >
```

**discovery/info\_disclosure/interesting\_files**

- Instale y cargue el complemento.

## Paso 2: Ejecute el nuevo módulo.

- Establezca la opción de origen en **hackxor.net** u otra ubicación de su elección. (Cumpla con los términos del curso al elegir un dominio). El sitio web h4cker.org también es interesante.
- Ejecute el comando. Este módulo crea un archivo .csv en la carpeta recon-ng/data.
- Busque el archivo y vea el contenido. Algunos de estos archivos se pueden descargar o ver mediante las URL en el resultado del comando.

```
[recon-ng][laboratorio] > workspaces select laboratorio
[recon-ng][laboratorio] > workspaces
Usage: workspaces <create|list|load|remove> [<name>]
[recon-ng][laboratorio] > marketplace install discovery/info_disclosure/interesting_files
[recon-ng][laboratorio] > modules search interesting_files
[recon-ng][laboratorio] > Reloading modules...
[recon-ng][laboratorio] > modules load discovery/info_disclosure/interesting_files
[recon-ng][laboratorio] > workspace Interesting_files > info
[recon-ng][laboratorio][Interesting_files] > info
  Name: Interesting File Finder
  Author: Tim Tomes (@Lannister5), thrapt (thrapt@gmail.com), Jay Turla (@hipcod3), and Mark Jeffery
  Version: 1.2
  Description:
    Checks hosts for interesting files in predictable locations.
  Options:
    Name Current Value Required Description
    CSV_FILE /home/kali/.recon-ng/data/interesting_files.verify.csv yes custom filename map
    DOWNLOAD True yes download discovered files
    PROTOCOL http yes request protocol
    SOURCE default yes source of input (see 'info' for details)
  Source Options:
    host     SELECT DISTINCT host FROM hosts WHERE host IS NOT NULL
    <string> string representing a single input
    <path> path to a file containing a list of inputs
    <query> database query returning one column of inputs
  Comments:
    * File Types: robots.txt, sitemap.xml,sitemap.xml.gz, crossdomain.xml,phpinfo.php,test.php,elmah.axd,server-status,3xx-console,admin-console,web-console
    * CSV Default: /home/kali/.recon-ng/data/interesting_files.verify.csv
    * Good Examples:
      - url:robots.txt ext:txt
      - url:elmah.axd ext:axd intitle:"Error log for"
      - url:server-status ext:html intitle:"Apache Status"
  [recon-ng][laboratorio][Interesting_files] > options set SOURCE hackxor.net
[recon-ng][laboratorio][Interesting_files] > info
  Name: Interesting File Finder
  Author: Tim Tomes (@Lannister5), thrapt (thrapt@gmail.com), Jay Turla (@hipcod3), and Mark Jeffery
  Version: 1.2
  Description:
    Checks hosts for interesting files in predictable locations.
  Options:
    Name Current Value Required Description
    CSV_FILE /home/kali/.recon-ng/data/interesting_files.verify.csv yes custom filename map
    DOWNLOAD True yes download discovered files
    PROTOCOL http yes request protocol
    SOURCE default yes source of input (see 'info' for details)
```

## Práctica de laboratorio: Uso de herramientas OSINT

```
[recon-ng][laboratorio][interesting_files] > options set SOURCE hackor.net
[recon-ng][laboratorio][interesting_files] > info
  Name: Interesting File Finder
  Author: Matt Tamas (BlameMaster53), thrapt (thrapt@gmail.com), Jay Turla (@shippcod3), and Mark Jeffery
  Version: 1.2
Description:
  Checks hosts for interesting files in predictable locations.

Options:
  Name      Current Value      Required   Description
  CSV_FILE  /home/kali/.recon-ng/data/interesting_files_verify.csv  yes        custom filename map
  DOWNLOAD  True                yes        download discovered files
  PORT      80                 yes        request port
  PROTOCOL http               yes        request protocol
  SOURCE    hackor.net          yes        source of input (see 'info' for details)

Source Options:
  default:  SELECT DISTINCT host FROM hosts WHERE host 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

Comments:
  * Files: robots.txt, sitemap.xml, sitemap.xml.gz, crossdomain.xml, phpinfo.php, test.php, elmah.axd,
  server-status, jmx-console/, admin-console/, web-console/
  * CSV Default: /home/Kali/.recon-ng/data/interesting_files_verify.csv
  * Google Dork: +intitle:"Error log for"
  * URLs:  -inurl:robots.txt ext:txt
           -inurl:elmah.axd ext:axd intitle:"Error log for"
           -inurl:server-status "Apache Status"

[recon-ng][laboratorio][interesting_files] > run
[recon-ng][laboratorio][interesting_files] > find -type f -iname "*robots.txt" found!
http://hackor.net:80/robots.txt => 404
[recon-ng][laboratorio][interesting_files] > find -type f -iname "*sitemap.xml" found!
http://hackor.net:80/sitemap.xml => 404
http://hackor.net:80/sitemap.xml.gz => 404
http://hackor.net:80/crossdomain.xml => 404
http://hackor.net:80/phpinfo.php => 404
http://hackor.net:80/test.php => 404
http://hackor.net:80/elmahtest.php => 404
http://hackor.net:80/admin-console/ => 404
http://hackor.net:80/jmx-console/ => 404
http://hackor.net:80/web-console/ => 404
[recon-ng][laboratorio][interesting_files] > 1 interesting files found.
[*] Files downloaded to '/home/kali/.recon-ng/worksheets/laboratorio/'
[recon-ng][laboratorio][interesting_files] >
```

```
[kali㉿kali]:~[-]
└─$ find -type f -iname "*interesting.csv" 2>/dev/null
/home/kali/.recon-ng/data/interesting_files_verify.csv

[kali㉿kali]:~[-]
└─$ find -type f -iname "*interesting.csv" 2>/dev/null
[sudo] password for kali:
[kali㉿kali]:~[-]
└─$ sudo find /usr -type f -iname "*interesting.csv" 2>/dev/null
[kali㉿kali]:~[-]
└─$ find -recon-ng -type f -iname "*csv" 2>/dev/null
/home/kali/.recon-ng/data/interesting_files_verify.csv

[kali㉿kali]:~[-]
```