

RECON-NG

¿Qué es Recon-ng?

Es una herramienta que nos permite recopilar información desde múltiples fuentes automatizando el proceso. Tiene una apariencia similar a [Metasploit](#), lo que reduce la curva de aprendizaje. Almacena los datos en bases de datos que luego se pueden consultar.

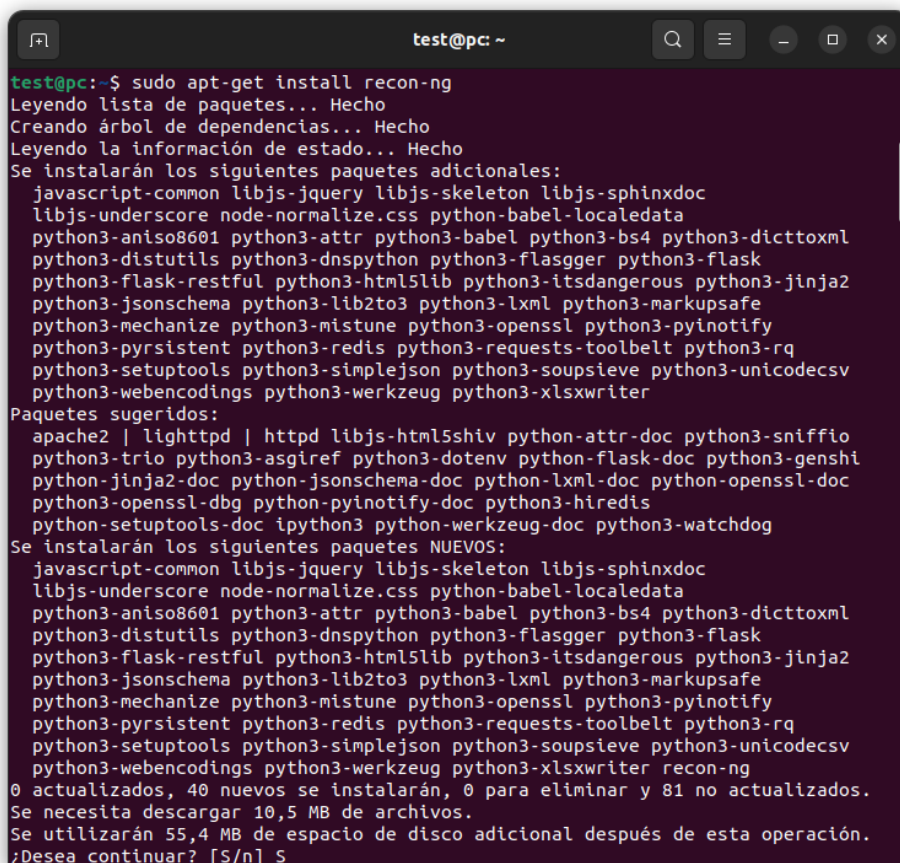
Instalación:

Vamos a instalarlo desde el repositorio, aunque también se puede instalar desde su [github](#).

Antes tenemos que actualizar:

```
sudo apt update -y && sudo apt dist-upgrade -y
```

```
sudo apt install recon-ng
```



```
test@pc: ~  
test@pc:~$ sudo apt-get install recon-ng  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes adicionales:  
  javascript-common libjs-jquery libjs-skeleton libjs-sphinxdoc  
  libjs-underscore node-normalize.css python-babel-localedata  
  python3-aniso8601 python3-attr python3-babel python3-bs4 python3-dicttoxml  
  python3-distutils python3-dnspython python3-flasgger python3-flask  
  python3-flask-restful python3-html5lib python3-itsdangerous python3-jinja2  
  python3-jsonschema python3-lib2to3 python3-lxml python3-markupsafe  
  python3-mechanize python3-mistune python3-openssl python3-pyinotify  
  python3-pyrsistent python3-redis python3-requests-toolbelt python3-rq  
  python3-setuptools python3-simplejson python3-soupsieve python3-unicodcsv  
  python3-webencodings python3-werkzeug python3-xlswriter  
Paquetes sugeridos:  
  apache2 | lighttpd | httpd libjs-html5shiv python-attr-doc python3-sniffio  
  python3-trio python3-asgiref python3-dotenv python-flask-doc python3-genshi  
  python-jinja2-doc python-jsonschema-doc python-lxml-doc python-openssl-doc  
  python3-openssl-dbg python-pyinotify-doc python3-hiredis  
  python-setuptools-doc ipython3 python-werkzeug-doc python3-watchdog  
Se instalarán los siguientes paquetes NUEVOS:  
  javascript-common libjs-jquery libjs-skeleton libjs-sphinxdoc  
  libjs-underscore node-normalize.css python-babel-localedata  
  python3-aniso8601 python3-attr python3-babel python3-bs4 python3-dicttoxml  
  python3-distutils python3-dnspython python3-flasgger python3-flask  
  python3-flask-restful python3-html5lib python3-itsdangerous python3-jinja2  
  python3-jsonschema python3-lib2to3 python3-lxml python3-markupsafe  
  python3-mechanize python3-mistune python3-openssl python3-pyinotify  
  python3-pyrsistent python3-redis python3-requests-toolbelt python3-rq  
  python3-setuptools python3-simplejson python3-soupsieve python3-unicodcsv  
  python3-webencodings python3-werkzeug python3-xlswriter recon-ng  
0 actualizados, 40 nuevos se instalarán, 0 para eliminar y 81 no actualizados.  
Se necesita descargar 10,5 MB de archivos.  
Se utilizarán 55,4 MB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] S
```

Iniciar:

Como podemos observar con la instalación tenemos tres interfaces. **Cli**: permite el uso desde la línea de comandos. **Ng**: interface recon. **Web**: reconocimiento basado en web.

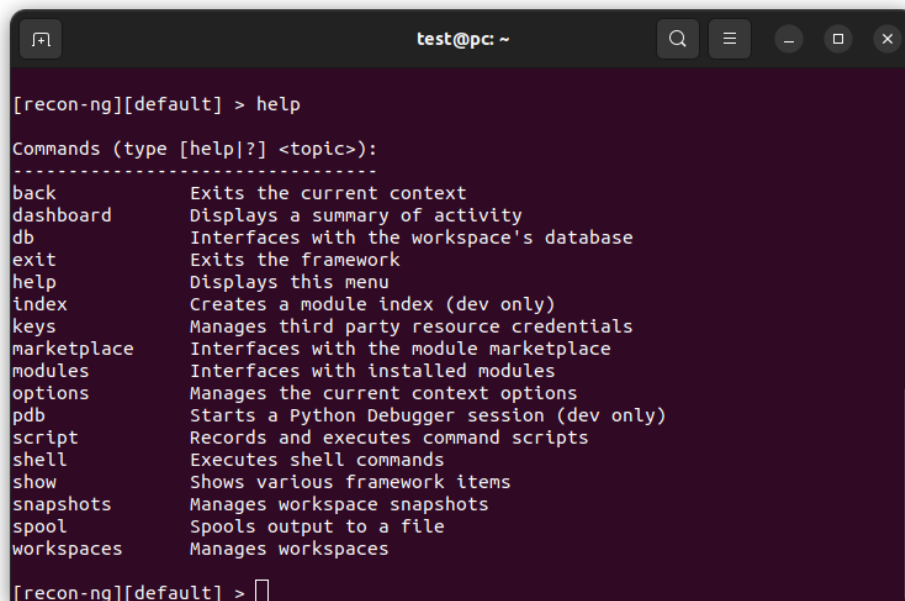
Escribimos el siguiente comando:

```
sudo recon-ng
```

[illegible][illegible]

Antes de empezar hay que ver que es lo que podemos hacer:

help



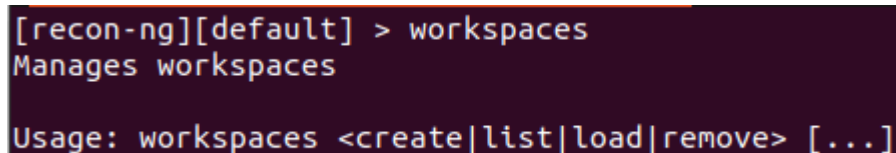
```
[recon-ng][default] > help
Commands (type [help|?] <topic>):
-----
back           Exits the current context
dashboard      Displays a summary of activity
db             Interfaces with the workspace's database
exit          Exits the framework
help          Displays this menu
index         Creates a module index (dev only)
keys          Manages third party resource credentials
marketplace   Interfaces with the module marketplace
modules       Interfaces with installed modules
options       Manages the current context options
pdb           Starts a Python Debugger session (dev only)
script        Records and executes command scripts
shell         Executes shell commands
show          Shows various framework items
snapshots     Manages workspace snapshots
spool         Spools output to a file
workspaces    Manages workspaces

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

Workspaces:

Recon nos permite trabajar con espacios de trabajo, para no mezclar información. Por defecto nos crea uno llamado default. Escribimos el siguiente comando:

workspaces



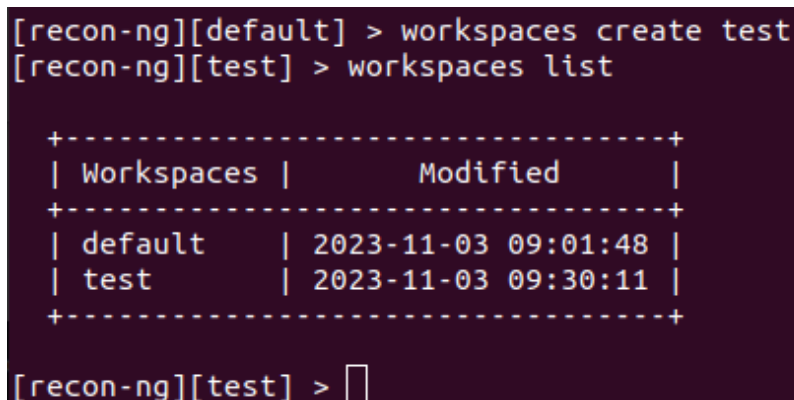
```
[recon-ng][default] > workspaces
Manages workspaces

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

Por defecto nos sitúa en default y al crear otro workspaces nos sitúa en el nuevo:

workspaces create test

workspaces list



```
[recon-ng][default] > workspaces create test
[recon-ng][test] > workspaces list

+-----+
| Workspaces |      Modified      |
+-----+
| default   | 2023-11-03 09:01:48 |
| test      | 2023-11-03 09:30:11 |
+-----+

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

Para volver a cambiar simplemente el comando *load* más el nombre:

workspaces load default

```
[recon-ng][test] > workspaces load default
[recon-ng][default] > 
```

Para borrar el comando *remove*:

workspace remove test

```
[recon-ng][default] > workspaces remove test
[recon-ng][default] > workspaces list

+-----+
| Workspaces |      Modified      |
+-----+
| default    | 2023-11-03 09:01:48 |
+-----+

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

Bases de datos:

Para poder consultar la información y ver los comandos escribimos:

db

```
[recon-ng][default] > db
Interfaces with the workspace's database

Usage: db <delete|insert|notes|query|schema> [...]

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

Podemos borrar, añadir, notas, consultar y ver. Para ver las tablas:

db schema

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

```
+-----+
| domains |
+-----+
| domain | TEXT |
| notes  | TEXT |
| module | TEXT |
+-----+

+-----+
| companies |
+-----+
| company | TEXT |
| description | TEXT |
| notes   | TEXT |
| module  | TEXT |
+-----+
```

Uso de claves:

Podemos cargar las *keys* de las API que tengamos de otros servicios como: Bing, Google...ect Para ello usaremos el siguiente comando:

```
keys
```

```
keys add {API Bing}
```

```
[recon-ng][default] > keys
Manages third party resource credentials

Usage: keys <add|list|remove> [...]

[recon-ng][default] > █
```

Ver información:

Para ver parte de la información almacenada, sólo tenemos que usar el comando *show*:

```
show
```

```
show credentials
```

```
[recon-ng][default] > show
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblo
cks|ports|profiles|pushpins|repositories|vulnerabilities>

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

Snapshots:

Podemos crear backups de los workspaces con el comando *snapshots*:

```
snapshots
```

```
snapshots take
```

```
[recon-ng][default] > snapshots
Manages workspace snapshots

Usage: snapshots <list|load|remove|take> [...]

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

¿Qué son los módulos?

Son herramientas que nos descargamos desde el Marketplace y que nos permite automatizar la tarea de recopilar información desde fuentes abiertas:

modules

```
[recon-ng][default] > modules
Interfaces with installed modules

Usage: modules <load|reload|search> [...]

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

¿Qué es el Marketplace?

Es una especie de repositorio con los módulos y versiones que podemos instalar:

marketplace

```
[recon-ng][default] > marketplace
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [...]

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

Para listar todos los módulos necesitamos el comando *search*:

marketplace search

```
[recon-ng][default] > 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	*	*
recon/companies-hosts/censys_tls_subjects	2.0	not installed	2021-05-11	*	*
recon/companies-multi/github_miner	1.1	not installed	2020-05-15		*

Podemos observar que tenemos información adicional:

- **Path:** Ruta y nombre del módulo
- **Versión:** Es la versión correspondiente
- **Status:** Si está instalada o no
- **Updated:** Fecha de la última modificación
- **D:** Si el módulo tiene dependencias
- **K:** Claves de terceros que tenemos que necesitamos para correr el módulo

Si queremos hacer una búsqueda más precisa:

marketplace search hackertarget

Para instalar:

marketplace install recon/domain-hosts/hackertarget

```
test@pc: ~  
[recon-ng][default] > marketplace search hackertarget  
[*] Searching module index for 'hackertarget'...  
  
+-----+  
| Path | Version | Status | Updated | D | K |  
+-----+  
| recon/domains-hosts/hackertarget | 1.1 | not installed | 2020-05-17 | | |  
+-----+  
  
D = Has dependencies. See info for details.  
K = Requires keys. See info for details.  
  
[recon-ng][default] > marketplace install recon/domains-hosts/hackertarget  
[*] Module installed: recon/domains-hosts/hackertarget  
[*] Reloading modules...  
[recon-ng][default] > modules search  
  
Recon  
-----  
recon/domains-hosts/bing_domain_web  
recon/domains-hosts/hackertarget  
  
[recon-ng][default] > █
```

A hora cargamos el módulo y vemos la información:

modules load recon/domain-hosts/hackertarget:

info

```
test@pc: ~  
[recon-ng][default] > modules load recon/domains-hosts/hackertarget  
[recon-ng][default][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 default yes source of input (see 'info' for details)  
  
Source Options:  
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL  
<string> string representing a single input  
<path> path to a file containing a list of inputs  
query <sql> database query returning one column of inputs  
  
[recon-ng][default][hackertarget] >
```

Para cambiar los valores con *options*:

options

```
[recon-ng][test][hackertarget] > options
Manages the current context options

Usage: options <list|set|unset> [...]

[recon-ng][test][hackertarget] >
```

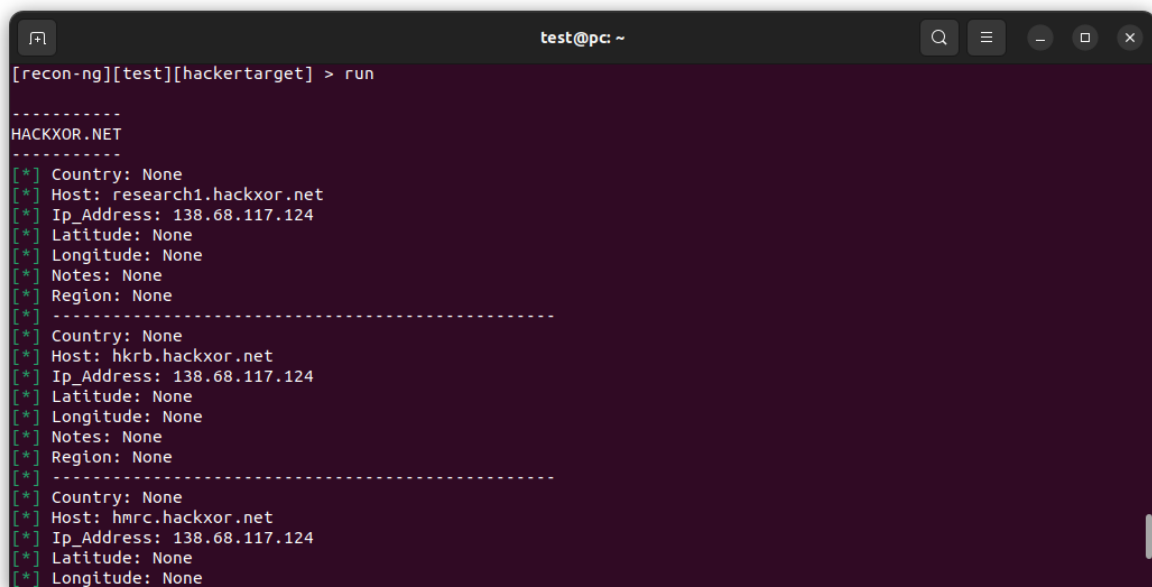
Cambiamos con *set*:

options set SOURCE hackxor.net

```
[recon-ng][test][hackertarget] > options set SOURCE hackxor.net
SOURCE => hackxor.net
[recon-ng][test][hackertarget] >
```

Finalizamos con *run*:

Run



```
test@pc: ~
[recon-ng][test][hackertarget] > run

-----
HACKXOR.NET
-----
[*] Country: None
[*] Host: research1.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: hkrb.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: hmrc.hackxor.net
[*] Ip_Address: 138.68.117.124
[*] Latitude: None
[*] Longitude: None
```

Para ampliar la información tenemos su [wiki](#)