

pdb	Inicia una sesión de Python Debugger (solo para desarrolladores)
script	Graba y ejecuta scripts de comando
shell	Ejecuta comandos de shell
show	Muestra varios elementos del marco
snapshots	Administra las instantáneas del espacio de trabajo.
spool	Carretes de salida a un archivo
workspaces	Administra espacios de trabajo

[recon-ng][default] > marketplace refresh este comando actualiza la base de datos

[recon-ng][default] > options list este comando lista las opciones por defecto.

Name	Current Value	Required	Description
NAMESERVER	8.8.8.8	yes	default nameserver for the resolver mixin
PROXY		no	proxy server (address:port)
THREADS	10	yes	number of threads (where applicable)
TIMEOUT	10	yes	socket timeout (seconds)
USER-AGENT	Recon-ng/v5	yes	user-agent string
VERBOSITY	1	yes	verbosity level (0 = minimal, 1 = verbose, 2 = debug)

[recon-ng][default] > workspaces create "achirou" Para crear un nuevo espacio de trabajo, utilice este comando.

[recon-ng][default] > workspaces list lista los espacios de trabajo que tenemos creados

```
+-----+
| Workspaces |
+-----+
| achirou   |
| default   |
+-----+
```

[recon-ng][default] > workspaces delete achirou para eliminar un espacio de trabajo utilizamos este comando

`recon-ng -w achirou2` con este comando puede abrir un espacio de trabajo en específico desde la consola

Para moverse entre los usuarios puede usar el siguiente comando.

`recon-ng][achirou2] > workspaces select achirou3` este comando cambiara de espacio de trabajo

NOTA IMPORTANTE El marco en sí no incluye ningún módulo por defecto. Los módulos deben instalarse desde el Marketplace de módulos. El comando `marketplace` proporciona esta capacidad, así como la capacidad de buscar, analizar y eliminar módulos. Al buscar módulos usando el `marketplace` CON EL subcomando `list`, es importante tomar nota de los módulos que requieren dependencias o credenciales de recursos de terceros, como lo señalan los asterisks en las columnas **D y K** de la salida. Utilizar el `marketplace info` MAS EL subcomando `<module>` para obtener una lista de las dependencias y / o credenciales requeridas, ya que deberán instalarse y / o agregarse manualmente antes de que el módulo funcione correctamente. La instalación de un módulo antes de que se cumplan sus dependencias generará mensajes de error al cargar y el módulo se colocará en estado "deshabilitado". La carga de un módulo antes de que se hayan agregado sus credenciales también dará como resultado un mensaje de advertencia sobre la falta de la clave, pero el módulo no se colocará en estado "deshabilitado" y probablemente fallará en el tiempo de ejecución debido a la imposibilidad de autenticar correctamente el recurso .

`[recon-ng][default] > marketplace search` con el siguiente comando podemos ver el listado de los modulos disponibles, y las dependencias o credenciales que se comentaban anteriormente

```
+-----+
|          Path          | Version |      Status      |
| Updated   | D  | K |
+-----+
| discovery/info_disclosure/cache_snoop          | 1.0     | not installed    | 2019-06-24 |
| |
| discovery/info_disclosure/interesting_files    | 1.0     | not installed    | 2019-06-24 | |
* |
| exploitation/injection/command_injector        | 1.0     | not installed    | 2019-06-24 | |
|
| exploitation/injection/xpath_bruter            | 1.1     | not installed    | 2019-08-19 |
| |*|
| import/csv_file                                | 1.1     | not installed    |
| 2019-08-09  | | |
```

```

| import/list | 1.0 | not installed
| 2019-06-24 | * |
| recon/contacts-contacts/mangle | 1.0 | not installed | 2019-06-24
| | |
| recon/contacts-contacts/unmangle | 1.0 | not installed | 2019-06-24
| | |
/////////*****
/

```

[recon-ng][default] > `modules search` este comando lista los modulos que ya tenemos instalados

```

Recon
-----
recon/domains-hosts/certificate_transparency
recon/domains-hosts/netcraft
[recon-ng][default] >

```

Cargar un modulo de la lista.

<https://achirou.com/>

Use este comando para instalar un modulo nuevo:

[recon-ng][achirou] > `marketplace install recon/profiles-profiles/profiler`

```
recon-ng][achirou] > marketplace search
```

```
[recon-ng][achirou] > modules load discovery/info_disclosure/interesting_files
```

```
[recon-ng][achirou][interesting_files] > info
```

Modificar las opciones

```
options set SOURCE achirou.com
```

Use este comando para ver los modulos que tiene instalados

```
[recon-ng][achirou][shodan_ip] > modules search
```

Recon

recon/domains-contacts/whois_pocs

recon/domains-hosts/shodan_hostname

recon/hosts-ports/shodan_ip

Use este comando para cambiar de modulos

[recon-ng][achirou][shodan_ip] > modules load recon/hosts-ports/shodan_ip

[recon-ng][default] > show

Shows various framework items

Usage: [show](#) el comando [show](#) nos muestra el listado de los comandos que podemos utilizar.

<companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default] > [show hosts](#) en este caso vamos a utilizar el comando **host** para ver el análisis que realizamos anteriormente

rowid	host	ip_address	region	country	latitude	longitude	module
1	www.achirou.com						certificate_transparency

Acá mostramos que no hay ningún dato almacenado bajo el **id** n **1**

[*] 1 rows returned

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

```
[*] No data returned.
```

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

```
[*] No data returned.
```

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

```
[*] No data returned.
```

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

```
[*] No data returned.
```

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

Agregar una api:

Con keys list podemos ver el listado de keys que tenemos instaladas

```
[recon-ng][achirou] > keys list
```

Ahora vamos a instalar una api keys para que vean el proceso. El comando es para agregar cualquier api keys: `keys add` seguido del nombre de la keys y la keys generada en este caso vamos a agregar la keys que nos brinda shodan

```
[recon-ng][achirou] > keys add shodan_api pnMQGV850QK6bNXgd2egb3RXCdQBf2YM
```

```
[*] Key 'shodan_api' added.
```

```
[recon-ng][achirou] > keys list
```

```
+-----+
| Name | Value |
+-----+
| shodan_api | pnMQGV850QK6bNXgd2egb3RXCdQBf2YM |
+-----+
```

Como se ve en el comando keys list, nos muestra la keys cargada con normalidad

