

* **TheHarvester:** <https://github.com/laramies/theHarvester>. Utiliza motores de búsqueda y otras bases de datos para recopilar información sobre un destino, como correos electrónicos, subdominios, hosts, nombres de empleados, puertos abiertos, etc. de varias fuentes públicas, servidores de claves PGP y la base de datos de computadoras SHODAN.

Es útil para los **evaluadores de penetración (penetration testers)** para comprender la huella del cliente en Internet y útil para cualquiera que quiera saber qué puede ver un atacante sobre su organización. Viene preinstalado en el KALI y PARROT, pero en caso de no estar se emplean los comandos siguientes:

- ✓ `git clone https://github.com/laramies/theHarvester.git`
- ✓ `cd theHarvester`
- ✓ `python3 -m pip install -r requirements.txt`
- ✓ `python3 ./theHarvester.py`

```
[vicky@parrot]-[~]
└─$ sudo git clone https://github.com/laramies/theHarvester.git
[sudo] password for vicky:
Clonando en 'theHarvester'...
remote: Enumerating objects: 13526, done.
remote: Counting objects: 100% (1256/1256), done.
remote: Compressing objects: 100% (333/333), done.
remote: Total 13526 (delta 1001), reused 1131 (delta 919), pack-reused 12270
Recibiendo objetos: 100% (13526/13526), 7.53 MiB | 7.23 MiB/s, listo.
Resolviendo deltas: 100% (8481/8481), listo.
```

```
[vicky@parrot]-[~]
└─$ cd theHarvester/
[vicky@parrot]-[~/theHarvester]
└─$
```

```
[vicky@parrot]-[~/theHarvester]
└─$ python3 -m pip install -r requirements.txt
ERROR: Introspect error on :1.65:/modules/kwalletd5: dbus.exceptions.DBusException: org.freedesktop.DBus.Error.NoReply: Message recipient disconnected from message bus without replying
WARNING: Keyring is skipped due to an exception: Failed to open keyring: org.freedesktop.DBus.Error.ServiceUnknown: The name :1.65 was not provided by any .service files.
Collecting aiodns==3.0.0
  Downloading aiodns-3.0.0-py3-none-any.whl (5.0 kB)
Collecting aiofiles==23.1.0
  Downloading aiofiles-23.1.0-py3-none-any.whl (14 kB)
```


Otra de las funcionalidades más interesantes es que permite exportar los resultados de cada búsqueda a archivos JSON y XML (esto lo realiza agregando el parámetro **-f nombre_de_archivo**) permitiendo la automatización en procesos de auditoría. Con la opción **-b all** se consigue una consulta completa.

🔗 Veamos unos ejemplos de comandos para obtener la información del sitio seleccionado:

- ❖ `theHarvester -d https://www.nhc.noaa.gov -l 500 -b all`
- ❖ `theharvester -d canarias7.es -l 500 -b google -f mis_resultados`
- ❖ `theharvester -d microsoft -l 200 -b linkedin`
- ❖ `theharvester -d apple.com -b googleCSE -l 500 -s 300`

VICTORIA EUGENIA PÉREZ GONZÁLEZ

Prof. J. Nefitoli

```
[x]-[vicky@parrot]-[~/theHarvester]
$python3 ./theHarvester.py -d https://www.nhc.noaa.gov -l 500 -b all
```

e*****

```
*                                                                 *  
* _|_|_||_||_||_||_||_||_||_||_||_||_||_||_||_||_||_||_||_||_||_*  
* | |_|_|_|_\/_/\_|\_/ \_/\_/ \_/\_/ \_/\_/ \_/\_/ \_/\_/ \_/\_/ \|_*  
* ||_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_*  
* \_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_*  
*                                                                *  
* theHarvester 4.4.1                                           *  
* Coded by Christian Martorella                                *  
* Edge-Security Research                                         *  
* cmartorella@edge-security.com                                 *  
*                                                                *
```

```
[*] Target: https://www.nhc.noaa.gov
```

[!] Missing API key for bevigil.

❖ Vamos a probar volcar los resultados en un fichero para crear un registro de un informe de auditoría:

❖ `theHarvester -d gobrunch.com -l 100 -b all -f fichero`

...Busca desde direcciones de correo electrónico de un dominio (-d gobrunch.com), limitando los resultados a 100 (-l 100), utilizando todas las búsquedas (-b all) para guardar el resultado en formato json y xml (-f <ruta al fichero>).

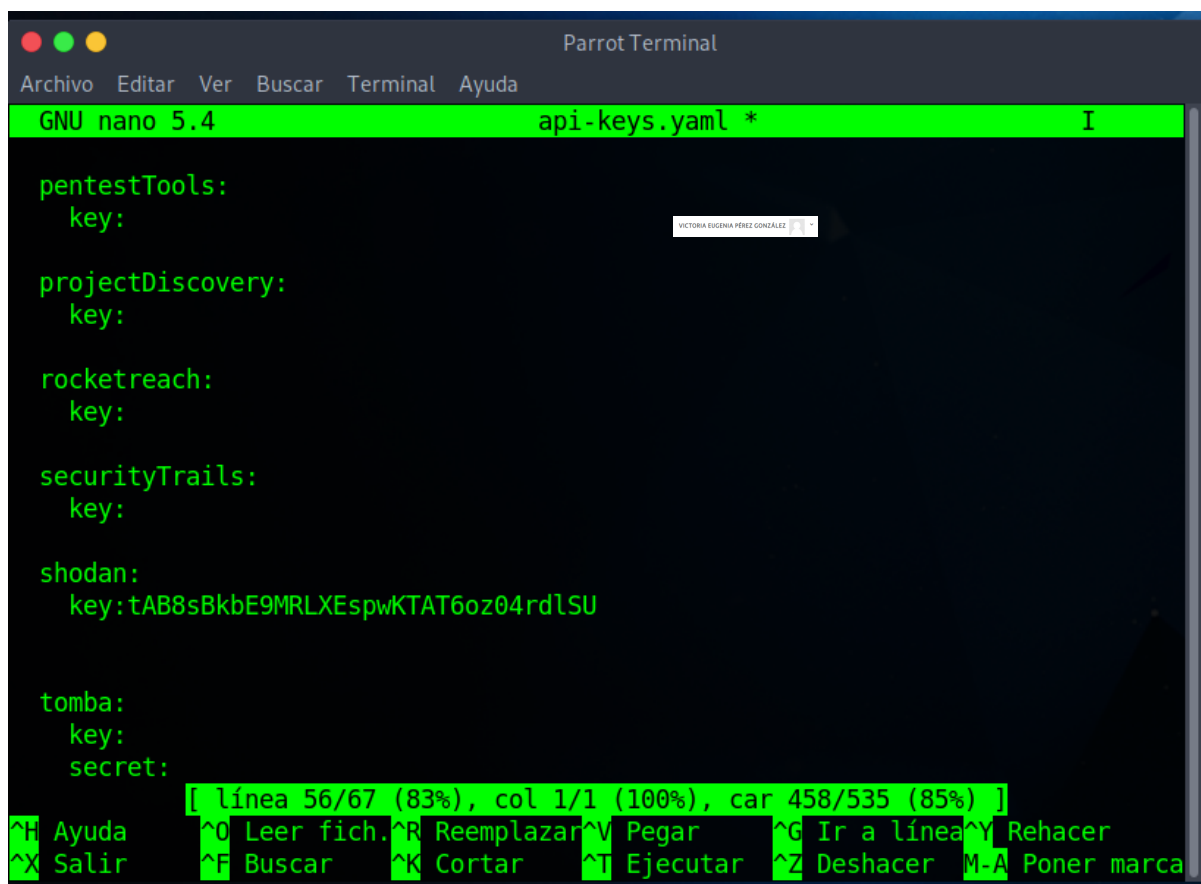
[illegible]

```
[*] Interesting Urls found: 4
-----
https://gobrunch.com/
https://gobrunch.com/auth/register?cfom=joinW0utRegistration&redirect=%2Ffbwly
https://gobrunch.com/auth/register?redirect=%2Fevents%2F211889%253Chttps%3A%2F%
Fnam11.safelinks.protection.outlook.com%2F%3Furl%3Dhttps%253A%252F%252Fgobrunch
com%252Fevents%252F211889%26data%3D04%25%25207C01%25%25207Cflavia.luiz%25%25204
owenscorning.com%25%25207C7282e3f20df14ae2ff2f08d9489294d6%25%25207C09e4e683c8e
4a8095d37f078d5a2649%25%25207C0%25%25207C0%25%25207C637620617252813149%25%25207
Unknown%25%25207CTWFpbGZsb3d8eyJWIjoimC4wLjAwMDAiLCJQIjoiv2luMzIiLCJBTiI6Ik1haw
iLCJXVCi6Mn0%25%25203D%25%25207C3000%2520%26%2520sdata%2520%3D%2520Na%25204%25%
5202FAMC8m25Fojyx0XSUHMGBYvNDqscxi1YD%25%25202FzU4hCI%25%25203D%2520%26%2520res
rved%2520%3D%25200%253E
https://www.blog.gobrunch.com/

[*] LinkedIn Links found: 0
-----

[*] IPs found: 34
-----
104.248.172.232
104.248.51.82
137.184.246.207
```

Añadir api key shodan.. en la carpeta de the harvester hay un archivo llamado api.keys.yaml



```
GNU nano 5.4 api-keys.yaml *

pentestTools:
  key:

projectDiscovery:
  key:

rocketreach:
  key:

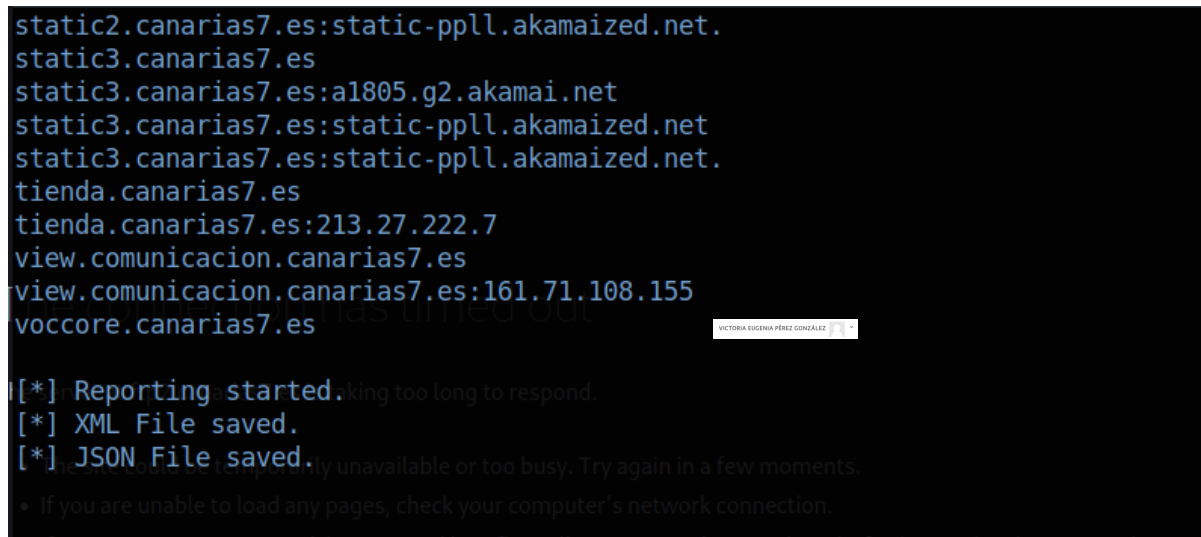
securityTrails:
  key:

shodan:
  key: tAB8sBkbE9MRLXEspwKTAT6oz04rdLSU

tomba:
  key:
  secret:

[ línea 56/67 (83%), col 1/1 (100%), car 458/535 (85%) ]
^H Ayuda ^O Leer fich. ^R Reemplazar ^V Pegar ^G Ir a línea ^Y Rehacer
^X Salir ^F Buscar ^K Cortar ^T Ejecutar ^Z Deshacer ^M-A Poner marca
```

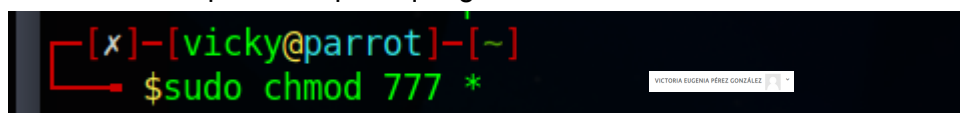
Se ejecuta de nuevo el escaneo



```
static2.canarias7.es:static-ppll.akamaized.net.
static3.canarias7.es
static3.canarias7.es:a1805.g2.akamai.net
static3.canarias7.es:static-ppll.akamaized.net
static3.canarias7.es:static-ppll.akamaized.net.
tienda.canarias7.es
tienda.canarias7.es:213.27.222.7
view.comunicacion.canarias7.es
view.comunicacion.canarias7.es:161.71.108.155
voccore.canarias7.es

[*] Reporting started. Taking too long to respond.
[*] XML File saved.
[*] JSON File saved.
If you are unable to load any pages, check your computer's network connection.
```

se cambian los permisos para que guarde el fichero



```
[x]-[vicky@parrot]-[~]
$ sudo chmod 777 *
```

```
[vicky@parrot]-(~/theHarvester)
$ls
api-keys.yaml      mypy.ini           requirements        theHarvester
bin                proxies.yaml       requirements.txt   theHarvester-logo.png
docker-compose.yml pyproject.toml     restfulHarvest.py theHarvester-logo.webp
Dockerfile         pytest.ini         setup.cfg          theHarvester.py
fichero.ison       README            setup.py          wordlists
fichero.xml        README.md         tests
```

```
Parrot Terminal
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
GNU nano 5.4 fichero.xml I
</host><host>www.canarias7.es</host><host>cartelera.canarias7.es</host><host>bl>
```

The connection has timed out

The server at ftp2.canarias7.es is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the