

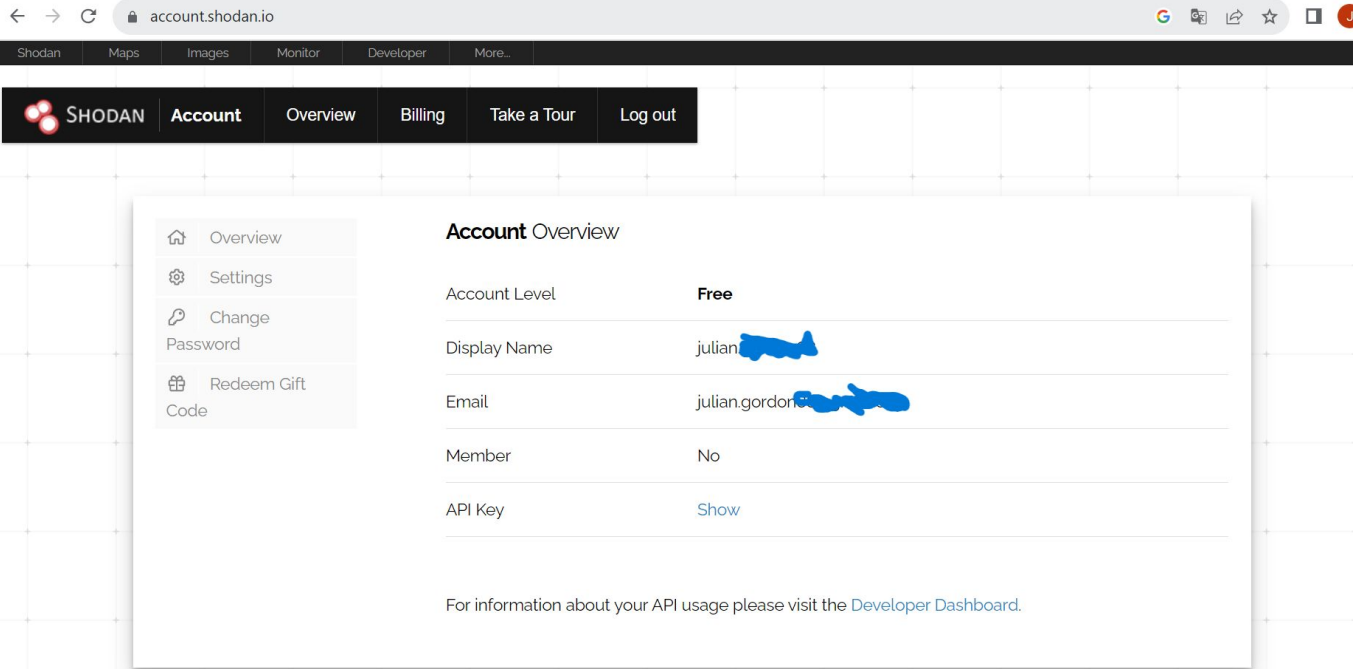


# **Curso de Hacking ético Master. D**

Ejercicio 1 - RECOPIACIÓN  
DE INFORMACIÓN

Alumno: Julián Gordon

Para crear una cuenta en Shodan, lo primero que debemos hacer es entrar a su pagina web shodan.io y seguir los pasos de registro. En la siguiente imagen se puede observar una captura de pantalla con los datos de mi cuenta creada



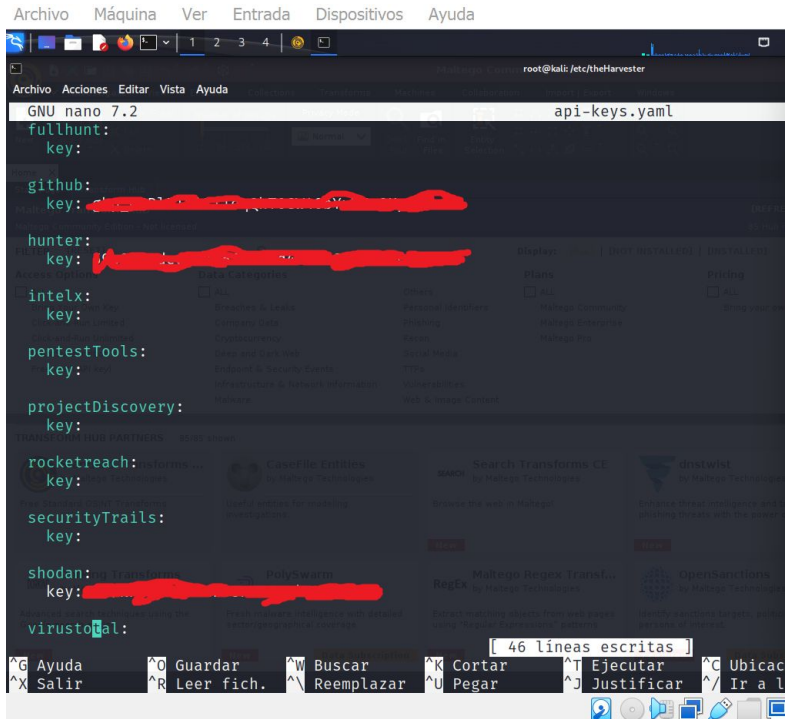
Para crear una cuenta en Hunter, los pasos son similares a los de Shodan. En la siguiente imagen se puede observar una captura de pantalla con los datos de registro y datos de la API key que usaremos para configurarlo luego.

The screenshot shows the Hunter.io web interface. The browser address bar displays 'hunter.io/api-keys'. The top navigation bar includes a search icon, a 'Search' button, and several tool icons: Finder, Verifier, Bulks, Leads, and Campaigns. On the right of the navigation bar, there is a user profile for 'Julian Gordon' on the 'Free plan'.

The main content area is divided into two sections. The top section is titled 'ACCOUNT & SETTINGS' and contains a sidebar with links to 'Account', 'Team', 'Subscription', 'Billing', 'Usage', 'Integrations', 'Add-ons', and 'API'. The 'API' link is currently selected. The main content of this section is titled 'API key' and features a '+ New key' button. Below this, there is a table with two columns: 'API KEY' and 'CREATED'. The table contains one entry with a masked API key ending in '910d', a copy icon, an eye icon, the creation date 'Sep 18, 2023 at 01:52 PM', and a 'Delete' link. A note below the table states: 'Your API keys are like your passwords: make sure to always keep them hidden! Share them only with services you trust.'

The bottom section is titled 'API overview' and includes a 'Full documentation' button. Below this, there is a 'Domain Search' section with a search bar.

Para configurar Shodan y Hunter en theHarvester, debemos agregar las API keys que logramos obtener cuando nos registramos en respectivas páginas web. Para ello, debemos abrir el archivo `api-keys.yaml` y agregarlas, para que la herramienta theHarvester pueda utilizarlos. Se puede observar en la siguiente imagen.



```
root@kali: /etc/theHarvester
GNU nano 7.2 api-keys.yaml
fullhunt:
  key:

github:
  key:

hunter:
  key:

intelx:
  key:

pentestTools:
  key:

projectDiscovery:
  key:

rocketreach:
  key:

securityTrails:
  key:

shodan:
  key:

virustoal:
  key:

[ 46 líneas escritas ]
Ayuda  Guardar  Buscar  Cortar  Ejecutar  Ubicac
Salir  Leer fich.  Reemplazar  Pegar  Justificar  Ir a l
```

En esta imagen se muestra un ejemplo de búsqueda sobre el dominio “hackthebox.eu”. TheHarvester, a través de Hunter, nos devuelve algunos correos electrónicos que encontró, asociados al dominio que usamos como objetivo

```
kali@kali: ~  
Archivo Acciones Editar Vista Ayuda  
└─$ theHarvester -d hackthebox.eu -b hunter  
*****  
*                               *  
* [TheHarvester]               *  
*                               *  
*                               *  
* theHarvester 4.2.0           *  
* Coded by Christian Martorella *  
* Edge-Security Research       *  
* cmartorella@edge-security.com *  
*                               *  
*****  
[*] Target: hackthebox.eu  
[*] Searching Hunter.  
[*] No IPs found.  
[*] Emails found: 10  
-----  
billing@hackthebox.eu  
community@hackthebox.eu  
dafd@hackthebox.eu  
education@hackthebox.eu  
goblin@hackthebox.eu  
info@hackthebox.eu  
legal@hackthebox.eu  
marketing@hackthebox.eu  
pr@hackthebox.eu
```

Ahora mostramos como configurar Shodan en Maltego, que es otra herramienta que se usa para la recopilación de información. Primero debemos buscar Shodan dentro de los Transforms e instalarlo.

The screenshot displays the Maltego Community Edition 4.4.1 interface. The top menu bar includes options like Investigate, View, Entities, Collections, Transforms, Machines, Collaboration, Import | Export, and Windows. Below the menu is a toolbar with various icons for file operations and search. The main window shows the 'Maltego Transform Hub' with a search filter set to 'shodan'. The results are categorized into several sections:

- Access Options:** Includes checkboxes for 'ALL', 'Bring Your Own Key', 'Click-and-Run Limited', 'Click-and-Run Unlimited', 'Data Subscription', and 'Free (with API key)'.
- Data Categories:** Includes checkboxes for 'ALL', 'Breaches & Leaks', 'Company Data', 'Cryptocurrency', 'Deep and Dark Web', 'Endpoint & Security Events', 'Infrastructure & Network Information', 'Malware', 'Others', 'Personal Identifiers', 'Phishing', 'Recon', 'Social Media', 'TTPs', 'Vulnerabilities', and 'Web & Image Content'.
- Plans:** Includes checkboxes for 'ALL', 'Maltego Community', 'Maltego Enterprise', and 'Maltego Pro'.
- Pricing:** Includes checkboxes for 'ALL' and 'Bring your own key'.
- Staff Picks:** Includes checkboxes for 'ALL', 'Cyber Security Operations', 'Government', and 'Trust & Safety'.
- Useful for Teams:** Includes checkboxes for 'ALL', 'Corporate Security & Business Risk', 'Counter-terrorism', 'Criminal Investigation', 'Cybercrime', 'Due Diligence', 'Financial Crime', and 'Fraud & Abuse'.

Below the search results, there is a section for 'TRANSFORM HUB PARTNERS' showing two partners: 'Shodan by Maltego Technologies' and 'Social Links CE by Social Links Inc. (Disclaimer)'. The Shodan partner description states: 'Shodan is the world's first search engine for Internet-connected devices. Query global IoT ...'. The Social Links CE partner description states: 'Free transforms (No API Key required) to retrieve data from ZoomEye, Shodan, SecurityTrails, ...'.

At the bottom, there is a section for 'INTERNAL HUB ITEMS' showing 0/0 shown.

Una vez lo tengamos instalado, debemos agregar la Api key que adquirimos al registrarnos.

Maltego Community Edition 4.4.1

InvestigateViewEntitiesCollectionsTransformsMachinesCollaborationImport | ExportWindows

New

Copy

Paste

Cut

Delete

Clear Graph

Number of Results

125025610k

Privacy Mode

Select All

Add Parents

Add Neighbors

Select Children

Select Bookmarked

Reverse Links

Zoom to Fit

Zoom In

Zoom Out

Zoom S

Home X

Start PageTransform Hub

Maltego Transform Hub

Maltego Community Edition - Not licensed

FILTER[RESET]shodan

Access Options

☐ ALL

☐ Bring Your Own Key

☐ Click-and-Run Limited

☐ Click-and-Run Unlimited

☐ Data Subscription

☐ Free (with API key)

Data Categories

☐ ALL

☐ Breaches & Leaks

☐ Company Data

☐ Cryptocurrency

☐ Deep and Dark Web

☐ Endpoint & Security Even

☐ Infrastructure & Network

☐ Malware

TRANSFORM HUB PARTNERS2/85 shown

Shodan

by Maltego Technologies

New and improved Transforms for querying Shodan. Supports vulnerability search as well as other advanced filtering ...

[REFRESH][DETAILS][UNINSTALL]

Soci

by So

Free transform data from Zoo

INTERNAL HUB ITEMS0/0 shown

Shodan

by Maltego Technologies

Bring Your Own KeyCounter-terrorismCybercrimeDeep and Dark WebFinancial CrimeIncident Response

Maltego CommunityMaltego EnterpriseMaltego ProPhishingVulnerabilities

Last modified: 27 March 2023

Shodan is the world's first search engine for Internet-connected devices. Query global IoT and Infrastructure data from within Maltego with these Transforms!

New and improved Transforms for querying Shodan. Supports

Shodan is the world's first search engine for Internet-connected the internet - whereas traditional search engines crawl the Wor Shodan aims to provide a complete picture.

With Maltego Transforms for Shodan, investigators are able to Maltego. These Transforms can be used with all tiers of Shoda

Pricing

Pricing Tier: Free Trial

Requirements: For full solution access, Maltego One, Classic or XL license and a Shodan API subscription

Access: There are two ways to access the Shodan Hub Item

- Free trial: Register for a free API key here <https://account.shodan.io/register>, and then download the Shodan Hub item in your Maltego Desktop Client and enter your trial key to begin accessing Shodan data using Maltego.
- Bring your own key: If you are an existing Shodan customer, simply download the Shodan Hub item in your Maltego Desktop Client and enter the paid API key to begin accessing Shodan data

View Certificate

Settings

Transform Seed Settings

Transform Inputs

Shodan API Key

Shodan API Key

Property ID: apiKey

Close

Una vez lo tengamos instalado y configurado, podemos hacer una búsqueda, por ejemplo, por el nombre de dominio y luego seleccionar Shodan para realizar esa búsqueda. En la siguiente imagen se muestra un ejemplo sobre el dominio “google.com”

The screenshot displays the Maltego Community Edition 4.4.1 interface. The main workspace shows a graph with a central node labeled 'google.com' (represented by a globe icon) and an outgoing link labeled 'To IP Addresses [Shodan]' pointing to a node labeled '142.250.191.206' (represented by a server icon). The interface includes a top menu bar, a toolbar with various actions like 'New', 'Copy', 'Paste', 'Clear Graph', and 'Delete', and a sidebar with 'Entity Palette' and 'Run View'. The 'Entity Palette' shows a search for 'dona' and a list of recently used entities including 'Domain', 'DNS Name', and 'Domain'. The 'Run View' shows a list of transforms, including 'Transform To DNS Records [Shodan]', 'Transform To DNS Records (from entity "google.com")', 'Transform To Subdomains (+ Historical) [Shodan]', 'Transform To Subdomains (+ Historical) (from entity "google.com")', 'Transform To IP Addresses [Shodan]', 'Transform To IP Addresses (from entity "google.com")', 'Transform To Tags [Shodan]', and 'Transform To Tags (from entity "google.com")'. The 'Output - Transform Output' pane at the bottom shows the results of the transforms, including the IP address 142.250.191.206. The 'Detail View' on the right shows the properties of the 'Domain' entity, including its type, domain name, and WHOIS info. The 'Property View' at the bottom right shows the properties of the 'Domain' entity, including its type, domain name, and WHOIS info.

FOR DEMO USE ONLY

Output - Transform Output

```
Transform To DNS Records [Shodan] returned with 0 entities (from entity "google.com")
Transform To DNS Records (from entity "google.com")
[403] Requires membership or higher to access (from entity "google.com")
Transform To Subdomains (+ Historical) [Shodan] returned with 0 entities (from entity "google.com")
Transform To Subdomains (+ Historical) (from entity "google.com")
Transform To IP Addresses [Shodan] returned with 1 entities (from entity "google.com")
Transform To IP Addresses (from entity "google.com")
[403] Requires membership or higher to access (from entity "google.com")
Transform To Tags [Shodan] returned with 0 entities (from entity "google.com")
Transform To Tags (from entity "google.com")
[403] Requires membership or higher to access (from entity "google.com")
```

Property View

Hub Transform Inputs	
Domain	
Type	Domain
Domain Name	google.com
WHOIS Info	
Graph Info	
Weight	0
Incoming	0
Outgoing	1
Bookmark	