

Censys: Motor de búsqueda sobre dispositivos y servidores en Internet

abril 19, 2016 [adastra](#) [Deja un comentario](#) [Go to comments](#)

Shodan es probablemente uno de los motores de búsqueda más utilizados por hackers (y curiosos) que quieren encontrar dispositivos y servidores en Internet que ejecutan servicios con características muy concretas, no en vano se le conoce como “el google de los hackers”. Es una herramienta muy valiosa que también permite acceder a sus funcionalidades de forma programática desde lenguajes de programación tales como Python, Perl o Ruby. En varias ocasiones se han mencionado sus virtudes en este blog y seguramente para muchos de vosotros nada de lo dicho anteriormente es algo nuevo, sin embargo cuando se menciona a “Censys”, actualmente son “pocas” las personas que conocen sus bondades. Del mismo modo que ocurre con Shodan, con Censys es posible realizar búsquedas muy concretas sobre dispositivos, servidores y redes que se encuentran en Internet, siendo un servicio muy similar y directa “competencia” de Shodan. El funcionamiento de Censys se basa en el uso de una herramienta que también es relativamente reciente y de la que [ya se ha hablado anteriormente en este sitio](#), se trata de Zmap un escaner que permite ejecutar un escaneo completo contra el rango de direcciones IPv4 y que con los recursos de computo adecuados, permite el escaneo entero de Internet en un tiempo bastante razonable. Se trata sin lugar a dudas de una herramienta que merece la pena estudiar y comprender. Censys se encarga de ejecutar escaneos con Zmap diariamente y recolecta información sobre los servicios que se encuentran disponibles en las direcciones IP analizadas, que como se ha dicho anteriormente, comprenden el rango de direcciones IPv4 entero. El creador de Censys es el mismo de Zmap (Zakir Durumeric) y desde el primer paper público sobre el uso de Censys, en octubre de 2015, tanto él como John Matherly (Shodan) han defendido a capa y espada sus respectivos sistemas como es natural, exponiendo las virtudes del uno sobre el otro. Después de estudiar ambos, personalmente no me decanto por uno solo, todo lo contrario, prefiero utilizar ambos para obtener más información y poder comparar/complementar resultados. Del mismo modo que ocurre con Shodan, es posible utilizar una API basada en servicios Rest que pueden ser consultados fácilmente si se tiene una “Developer Key”, la cual se puede conseguir simplemente creando una cuenta gratuita en el servicio. Todos los días es posible acceder a un snapshot de los datos recolectados por el servicio, indicando la información disponible sobre direcciones, puertos, sitios web, certificados, etc. Por otro lado, la API está compuesta por los siguientes endpoints.

search	Permite ejecutar búsquedas contra los índices más recientes que ha recolectado el sistema.
view	Permite recuperar información sobre un host concreto, sitio web o certificado.
report	Permite generar un reporte agrupado sobre un campo concreto en el conjunto de resultados.
query	Permite la ejecución de una consulta SQL contra la información actual e histórica que se ha ido registrando en el sistema y únicamente está disponible a investigadores verificados.

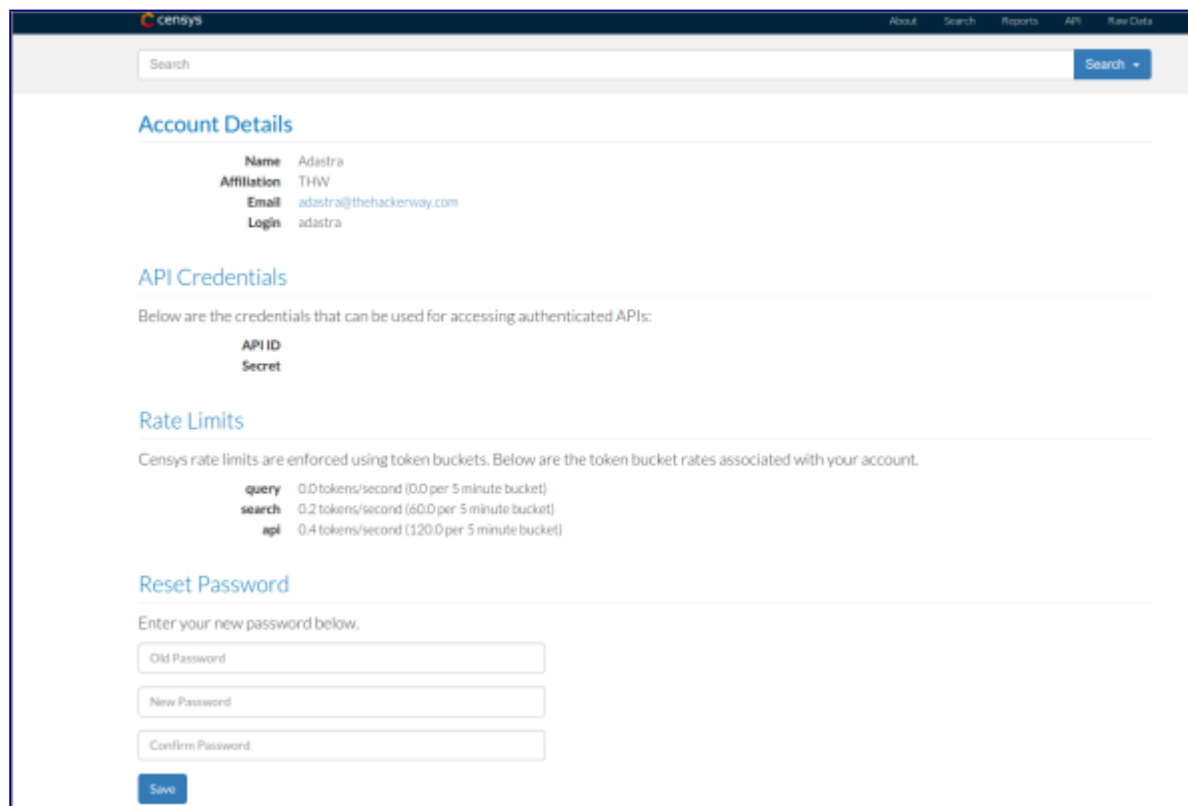
export

Permite la exportación de un conjunto de registros en formato JSON

data

Expone metadatos sobre la información en formato “crudo” que es recolectada diariamente por el sistema.

Como se puede apreciar, son muy pocos endpoints y no es una API tan completa como la que implementa Shodan, pero sigue siendo muy interesante por la información que aporta. En este punto es posible interactuar con Censys por medio de dichos endpoints de forma programática, para ello es necesario crear una cuenta en Censys y obtener los campos API ID y Secret, tal como se puede apreciar en la siguiente imagen.



The screenshot shows the Censys web interface. At the top, there is a navigation bar with links for 'About', 'Search', 'Reports', 'API', and 'Rate Data'. Below the navigation bar is a search bar with a 'Search' button. The main content area is divided into several sections:

- Account Details:** This section displays the user's account information:
 - Name: Adastra
 - Affiliation: THW
 - Email: adastra@thehackerway.com
 - Login: adastra
- API Credentials:** This section provides the credentials for accessing authenticated APIs:
 - API ID
 - Secret
- Rate Limits:** This section shows the token bucket rates associated with the account:
 - query: 0.0 tokens/second (0.0 per 5 minute bucket)
 - search: 0.2 tokens/second (60.0 per 5 minute bucket)
 - api: 0.4 tokens/second (120.0 per 5 minute bucket)
- Reset Password:** This section contains a form to reset the password, with fields for 'Old Password', 'New Password', and 'Confirm Password', and a 'Save' button.

A la fecha de redactar este documento no hay ningún tipo de cliente oficial para Censys, pero dado que se trata de un servicio que se expone por medio de una API Rest, es posible utilizar cualquiera de las librerías disponibles en lenguajes de programación como Python, Ruby, C o Java, para consumir dichos servicios Rest sin mayores dificultades. En este caso concreto y tal como se ha visto en varias ocasiones en este blog, se utilizará Python para crear un cliente básico que consuma algunos de los servicios disponibles en Censys.

```

1 import sys
2 import json
3 import requests
4 API_URL = "https://www.censys.io/api/v1"
5 UID = "xxxxxx"
6 SECRET = "zzzzz"
7 res = requests.get(API_URL + "/data", auth=(UID,
8 SECRET))
9 if res.status_code != 200:
10     print "error occurred: %s" % res.json()["error"]
11     sys.exit(1)
12 for name, series in res.json()["raw_series"].iteritems():
13     print series["name"], "was last updated at",
14         series["latest_result"]["timestamp"]
15 params = json={"query": "Apache",
16 "page": 1}
17 res = requests.post(API_URL + "/search/certificates",
18 auth=(UID, SECRET), json=json)
19 print res.json()["results"][0].keys()
20 print res.json()["results"][0].values()

```

Hay que tener en cuenta que de acuerdo a la documentación la API Rest de Censys, es necesario invocar a cada uno de los endpoints con un método HTTP concreto, una serie de parámetros obligatorios y que además, muchas de las peticiones reciben datos en formato JSON, con lo cual es necesario realizar las peticiones HTTP siguiendo estas especificaciones. El script anterior es simplemente un ejemplo sobre el uso de los endpoints “/data” y “/search/certificates”. Tal como se puede apreciar, es bastante sencillo crear un cliente y obtener información de Censys utilizando su API Rest.

De todos modos, desde mi punto de vista hay dos características que hacen que Shodan sea una buena opción con respecto a Censys, considerando nuevamente que a mi juicio es recomendable utilizar ambas.

1. La API de Shodan parece estar mejor documentada y ser más completa, además de que hay clientes en diferentes lenguajes, lo que facilita su integración en cualquier herramienta, esto a la fecha de redactar este documento, no se consigue con Censys.

- 2- Shodan cuenta con varios filtros que permiten afinar las búsquedas y a la fecha de redactar este artículo, son mucho más completos que los que se encuentran disponibles en la interfaz de búsqueda de Censys.

En contrapartida, Censys permite el acceso a la información histórica que se ha ido recolectado y no pone limitaciones sobre los tipos de servicios que se pueden consultar, algo que si hace Shodan.

Se trata simplemente de un servicio que podéis utilizar de forma complementaria a Shodan para la recolección de información, se perfila como una excelente herramienta para ejecutar procesos OSINT y análisis de datos.

Un saludo y Happy Hack!