

[thecryptocuy.io](https://thecryptocuy.io)

# Tutorial de Shodan, el inicio de un análisis pasivo -

*Mendax*

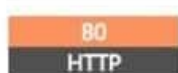
4-5 minutos

---

## Qué es Shodan?

Shodan es un motor de búsqueda para encontrar dispositivos específicos y tipos de dispositivos que existen en línea. Las búsquedas más populares son cosas como webcam, linksys, cisco, netgear, SCADA, etc.

Funciona escaneando todo Internet y analizando los banners que son devueltos por varios dispositivos. Utilizando esa información, Shodan puede decirnos cosas como qué servidor Web y qué versión es más popular, o cuántos servidores FTP anónimos existen en una ubicación en particular y qué marca y modelo puede ser el dispositivo.

  
**Apache httpd**

```
HTTP/1.1 301 Moved Permanently
Date: Wed, 13 May 2015 11:28:04 GMT
Server: Apache
Set-Cookie: symfony=ilam76d0vps16i9fqjth9in5i4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: http://google.com
Vary: Accept-Encoding
Content-Length: 0
Connection: close
Content-Type: text/html; charset=utf-8
```

Shodan es de uso particular para la investigación de seguridad en Internet de las cosas (IoT), ya que pronto habrá miles de millones de dispositivos en línea que tienen vulnerabilidades específicas que deben repararse y pueden identificarse rápidamente por su información de banner.

## Bases

Empezamos navegando a la página principal y luego ingresando en el campo de búsqueda, como lo haría con cualquier otro motor de búsqueda.

Para ello podemos buscar por ejemplo “VNC”

Exploits Maps Download Results Create Report

**TOP COUNTRIES**

Showing results 1 - 10 of 754

**197.81.147.64**  
 197.81.147.64, South Africa  
 NWES  
 Accessed on 2015-05-12 12:13 GMT  
 Details

**194.69.36.22**  
 194.69.36.22, Europe  
 Luthie Luthie GmbH  
 Accessed on 2015-05-12 10:38 GMT  
 Details

**50.116.54.161**  
 50.116.54.161, United States  
 Linux  
 Accessed on 2015-05-12 11:20 GMT  
 Details

**46.105.113.91**  
 46.105.113.91, France  
 OVN SAS  
 Accessed on 2015-05-12 10:54 GMT  
 Details

**152.44.111.79**  
 152.44.111.79, United States  
 Gardiner-Webb University  
 Accessed on 2015-05-12 10:42 GMT  
 Details

**TOP SERVICES**

SSH 242  
 VNC 206  
 China 79  
 VNC (RDP) 70  
 SSH 68

**TOP ORGANIZATIONS**

Deutsche Telekom AG 38  
 Gardiner-Webb University 38  
 Luthie Luthie GmbH 23  
 Comcast Cable 8  
 China Telecom nongda 8

**TOP OPERATING SYSTEMS**

Linux 3.x 8  
 Windows 7 or 8 8  
 Windows XP 3  
 Linux 2.6.x 1

**TOP PRODUCTS**

RealVNC 81  
 OpenSSH 45  
 VNC Server Enterprise Ed... 26  
 Apache httpd 20  
 Dropbear sshd 8

HTTP/1.1 400 Bad Request  
 Date: Wed, 12 May 2015 12:05:26 GMT  
 Server: Apache  
 Expires: Thursday, 01-Jan-1970 00:00:01 GMT  
 Pragma: no-cache  
 X-Frame-Options: SAMEORIGIN  
 Vary: Accept-Encoding  
 Connection: close  
 Content-Type: text/html; charset=utf-8

<!DOCTYPE html>  
 PUBLIC "-//W3C//DTD HTML 4...

SSH-2.0-OpenSSH\_6.6.1p1 Ubuntu-2ubuntu2  
 Key type: ssh-rsa  
 Key: AAAAB3NzaC1yc2EAAAADAQABAAQDQ0bip1J1Hw/3QWQ0d5/3eQjcc5L8ypCtdGFH3/9bV2Mk  
 VmH1q3oqkyLies/DofTH+d7b/tZ4nFuYK3ZmP1S9uHNEY18Cv+S2EXG1MOPaQ4tcVqCFrDNP  
 PL1wXV3H4r6da9HcS2zQL/q+/W/fq588kgPmg4d7/aSYTRx473HcQj1E1naQ7VW0A12xyR0d  
 SER...

SSH-2.0-OpenSSH\_5.8p1 Debian-4+deb7u2  
 Key type: ssh-rsa  
 Key: AAAAB3NzaC1yc2EAAAADAQABAAQDQ0bip1J1Hw/3QWQ0d5/3eQjcc5L8ypCtdGFH3/9bV2Mk  
 Aboc4/3jM3dp3XxPk3APjgkj1P9H5G8pRfwr2athY1aH80QpQo1bgtJRTzokTranBS1yAYLp8  
 yeFmx0qprf9wr1Q10Ku37aDrc4tevrHtyc0k+1Vw9H5321/a9334F1PwJH8uo7CFv8l0zj/VNw  
 1QC1V...

HTTP/1.1 200 OK  
 Content-Type: text/html; charset=utf-8  
 Content-Length: 3533  
 Connection: Close

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">  
 <html>  
 <head>  
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">  
 <title>  
 Application Control Vista...

A partir de este resultado, podemos pasar a algunas áreas clave en los resultados. Comenzando en la barra lateral izquierda, vemos

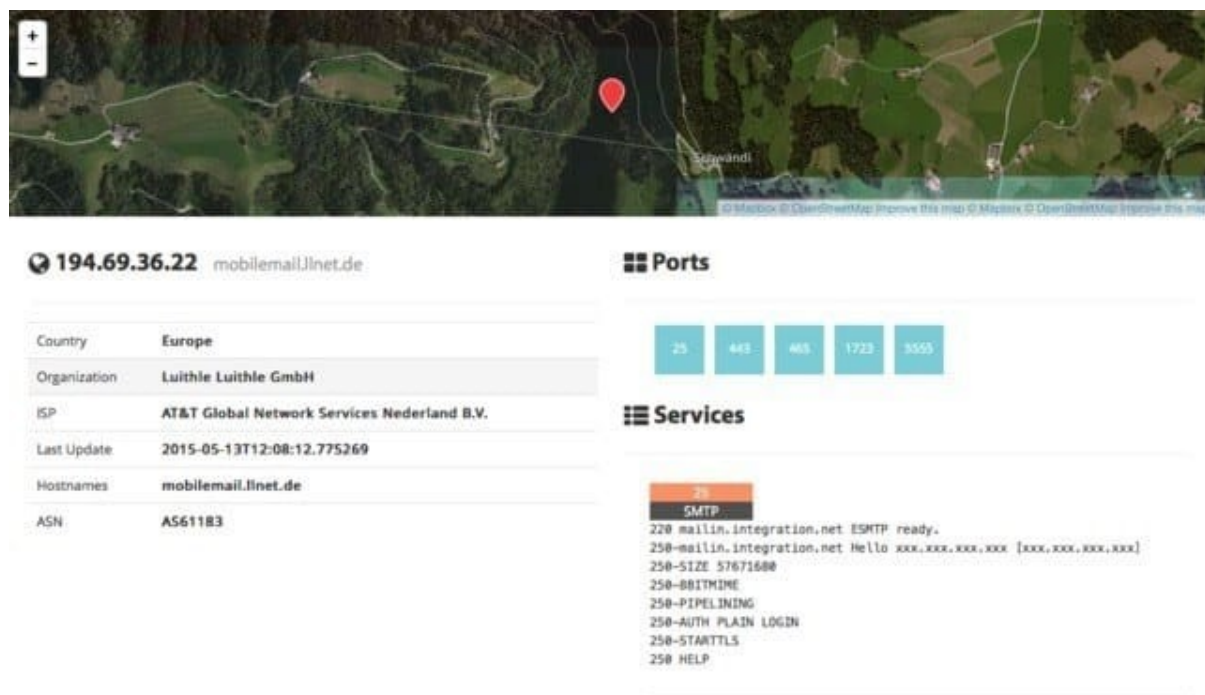
una buena cantidad de datos de resumen:

- Mapa de resultados.
- Top de servicios (puertos)
- Top de organizaciones (ISP)
- Top de sistemas operativos.
- Top de productos (software)

Luego, en la sección principal, obtenemos la lista de resultados completa, que incluye:

- Dirección IP
- Nombre del host.
- IPS.
- Cuando se agregó la entrada a la Base de Datos.
- El país en el que se encuentra.

Para obtener aún más información, se puede hacer click en los detalles, que nos llevará al host en sí:



**194.69.36.22** mobilemail.llnet.de

Country	Europe
Organization	Luithe Luithe GmbH
ISP	AT&T Global Network Services Nederland B.V.
Last Update	2015-05-13T12:08:12.775269
Hostnames	mobilemail.llnet.de
ASN	AS61183

**Ports**

25 443 465 1723 3555

**Services**

25 SMTP

```
220 mailin.integration.net ESMTTP ready.
250-mailin.integration.net Hello xxx.xxx.xxx.xxx [xxx.xxx.xxx.xxx]
250-SIZE 57671680
250-8BITIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
```

Aquí podemos ver los datos sobre el host a la izquierda, la lista de

los puertos que se encontraron en la parte superior derecha y luego los detalles de los puertos y descripción de cada puerto a medida que avanzamos por la página.

## Uso de filtros

Como con cualquier motor de búsqueda, Shodan funciona bien con búsquedas básicas de un solo término, pero el verdadero poder viene con consultas personalizadas.

Estos son los filtros de búsqueda básicos que podemos utilizar:

- City: Encuentra dispositivos en un ciudad particular.
- Country: Encuentra dispositivos en un país particular.
- geo: Se puede incluir coordenadas.
- hostname: Encuentra valores que coincidan con el nombre de host.
- net: Búsqueda basada en una IP o CIDR
- os: Búsqueda basada en el sistema operativo.
- port: Encuentra puertos específicos que estén abiertos.
- Before/after: Encuentra resultados dentro de un período de tiempo

## Por ejemplo:

Encontrar servidores apache en Cuenca-Ecuador:

```
apache city:"Cuenca" country:"EC"
```

Encontrar Nginx servers en Alemania:

```
Nginx country:"DE"
```

Encontrar servidores GWS:

```
"server:gws" hostname:"google"
```

Encontrar dispositivos Cisco con una subred en particular:

```
cisco net:"216.219.143.0/24"
```

Así que, básicamente tenemos un conjunto de términos para realizar búsquedas de dispositivos que estemos buscando.

## Casos de uso

Podemos usar el botón “Explore” en el sitio principal de Shodan para ver búsquedas y resultados comunes, que son esclarecedores.

Encontraremos cosas como:

1. Cámaras Web.
2. SCADA.
3. Semáforos.
4. Routers.
5. Contraseñas predeterminadas, etc.

Es bastante interesante buscar en la red, pero también un poco aterrados, (cámaras web!).

Para combinar filtros, simplemente hay que seguir agregándolos. También podemos hacer eso haciendo click en los filtros en la barra lateral izquierda para un conjunto de resultados determinado. Entonces, si desea buscar servidores Nginx en Quito, que se ejecutan en el puerto 8080, que también ejecutan Tomcat, puede hacerse de la siguiente manera:

```
Apache city:"Quito" country:"EC" port:"8080"  
product:"Apache tomcat/Coyote JSP engine"
```

## Uso avanzado

Aquí hay algunas otras cosas interesantes que se pueden hacer con el servicio.

- Exportación de datos: Podemos exportar los resultados en varios formatos utilizando el menú superior después de haber realizado una búsqueda.
- Búsqueda de navegador: Podemos configurar en su navegador para buscar Shodan cuando busca desde la barra de URL.
- Cuentas premium: Una cuenta premium es un pago único de \$45 y le brinda un mayor acceso a la API. Los detalles complementos y los documentos están disponibles en <https://developer.shodan.io>.