

Shodan

Shodan was created by computer scientist John Matherly as a hobby. Matherly wanted to track any type of device connected to the internet. This is how Shodan became real in 2009.

Shodan indexation works by searching open ports of any service or device. This means that Shodan, unlike any normal search engine, does not focus on searching web pages but on collecting the banners of the services (server response to a request). These services include HTTP, HTTPS, FTP, SSH, Telnet, SNMP and SIP protocols. Then, the user can search for devices by regions or geographic areas applying Shodan filters.

How Shodan works

Basically, Shodan tracks public access devices, preferably in SCADA systems (Supervisory Control and Data Acquisition). SCADA systems are used to control and supervise industrial processes remotely in real time.

Shodan uses automated search tools that allow massive queries. One of these tools is Shodan Diggity. This tool is powered by a database known as Shodan Hacking Database that works as a kind of dictionary to locate different devices connected to the internet: printers, webcams, routers, transit systems and, of course, industrial control systems.

Shodan Web Interface: Shodan's web interface is a search engine for internet-connected devices, offering insights into their vulnerabilities and configurations. Users can search by criteria like location, device type, and software, accessing data on open ports, services, and potential security risks, facilitating network monitoring and research.

Shodan Web Queries:

1. Port: Port keyword is used to scan for the ports. Here I used port 22 to watch SSH ports.

The screenshot displays the Shodan web interface with a search query of 'port:22'. The interface is dark-themed and includes a navigation bar at the top with links for Shodan, Maps, Images, Monitor, Developer, and More. The search bar contains the query 'port:22' and a search button. Below the search bar, the total number of results is 27,627,880. The left sidebar shows a world map and a list of top countries with their respective result counts: United States (7,388,708), Brazil (2,908,162), China (2,747,014), Germany (2,159,797), and Argentina (1,209,592). The main content area displays three search results for the query 'port:22'. Each result includes a company name, a key, and a timestamp. The first result is for '43.153.210.239' with a key 'SSH-2.0-OpenSSH_7.4' and a timestamp of '2024-05-07T22:20:58.517000'. The second result is for '143.110.230.199' with a key 'SSH-2.0-OpenSSH_7.4' and a timestamp of '2024-05-07T22:24:38.667000'. The third result is for '119.45.100.167' with a key 'SSH-2.0-OpenSSH_8.0' and a timestamp of '2024-05-07T22:24:29.557148'.

Country	Count
United States	7,388,708
Brazil	2,908,162
China	2,747,014
Germany	2,159,797
Argentina	1,209,592

Company	Key	Timestamp
43.153.210.239	SSH-2.0-OpenSSH_7.4	2024-05-07T22:20:58.517000
143.110.230.199	SSH-2.0-OpenSSH_7.4	2024-05-07T22:24:38.667000
119.45.100.167	SSH-2.0-OpenSSH_8.0	2024-05-07T22:24:29.557148

2. Os: This is used to search for operating system.

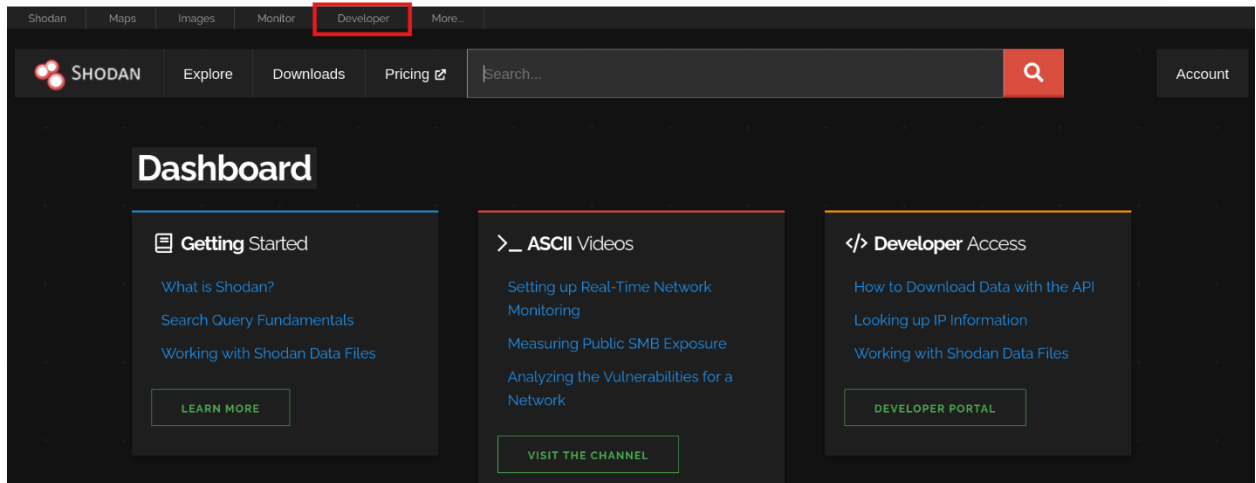
The screenshot shows the Shodan search interface with the query 'os:windows 10'. The results page displays 2,708,296 total results. On the left, there are sections for 'TOP COUNTRIES' and 'TOP PORTS'. The 'TOP COUNTRIES' section shows a world map and a list of countries with their respective result counts: United States (602,493), China (492,757), Germany (163,322), Hong Kong (91,347), and Korea, Republic of (86,409). The 'TOP PORTS' section shows a list of ports with their respective result counts: 3389 (1,374,042), 80 (350,501), 443 (238,323), and 1433 (201,030). The main results area shows three entries. The first entry is for IP 1.12.230.140, associated with Tencent Cloud Computing (Beijing) Co., Ltd. in China, Shenzhen. It shows an SSL Certificate and Remote Desktop Protocol (RDP) information. The second entry is for IP 84.45.41.215, associated with CloudCock Connected Limited in the United Kingdom, London. It shows an HTTP/1.1 200 OK response. The third entry is for IP 2.35.82.239, associated with Vodafone Italia S.p.A. in Italy. It shows an SSL Certificate and Remote Desktop Protocol (RDP) information.

3. Port: Port keyword is used to scan for the ports. Here I used port 3389 to watch RDP ports.

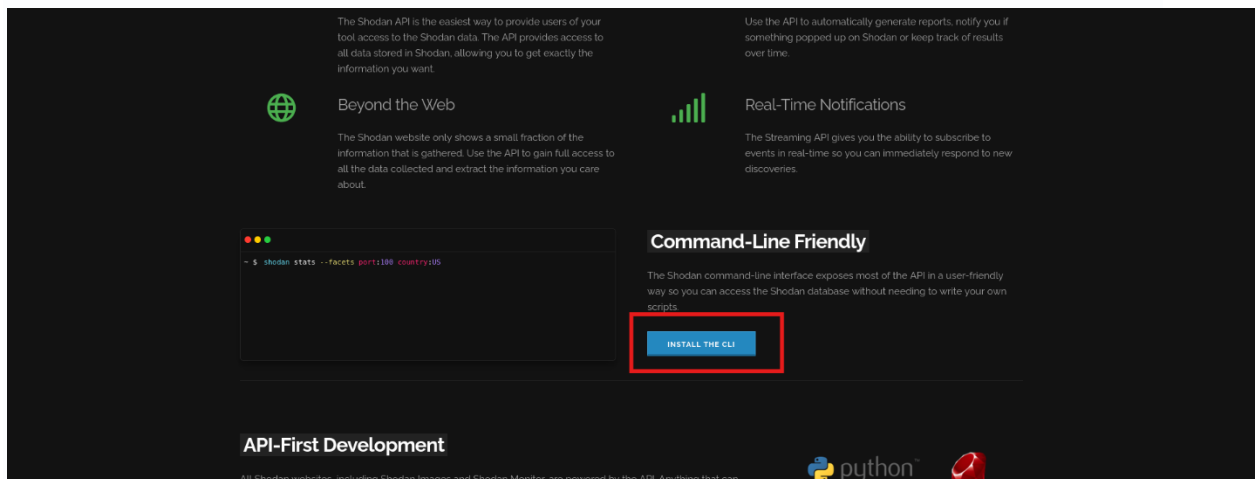
The screenshot shows the Shodan search interface with the query 'port:3389'. The results page displays 4,699,596 total results. On the left, there are sections for 'TOP COUNTRIES' and 'TOP ORGANIZATIONS'. The 'TOP COUNTRIES' section shows a world map and a list of countries with their respective result counts: China (1,637,811), United States (1,224,823), Germany (215,108), Japan (123,171), and Hong Kong (119,590). The 'TOP ORGANIZATIONS' section shows a list of organizations with their respective result counts: Tencent cloud computing (Beijing) Co., Ltd. (460,321), Google LLC (397,554), Aliyun Computing Co., LTD (325,108), and Tencent Cloud Computing (Beijing) Co., Ltd. (314,409). The main results area shows three entries. The first entry is for IP 2a02:e980:d::5399, associated with Equinix Inc. in the United States, San Mateo. It shows an HTTP/1.1 400 Bad Request response. The second entry is for IP 34.149.98.168, associated with Google LLC in the United States, Kansas City. It shows 'No data returned'. The third entry is for IP 43.142.44.198, associated with Tencent Cloud Computing (Beijing) Co., Ltd. in China, Shanghai. It shows an SSL Certificate and Remote Desktop Protocol (RDP) information.

Shodan CLI Downloading steps:

1. Firstly, go to Shodan Dashboard and click on **Developer** option from the task bar.



2. Now click on the **Install The CLI** Button.



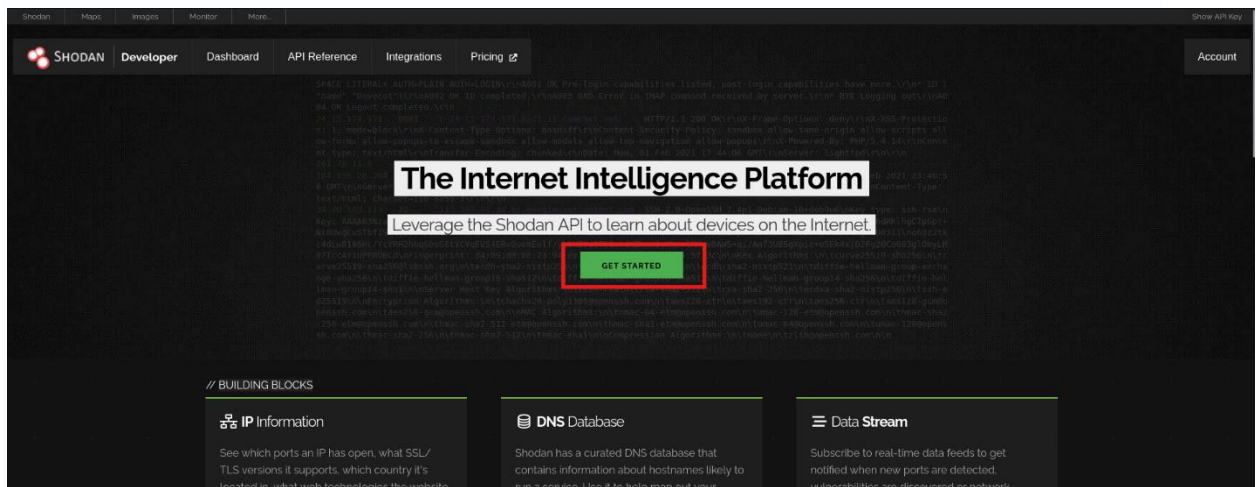
```
(root@kali)-[/home/kali]
# shodan

Usage: shodan [OPTIONS] COMMAND [ARGS]...

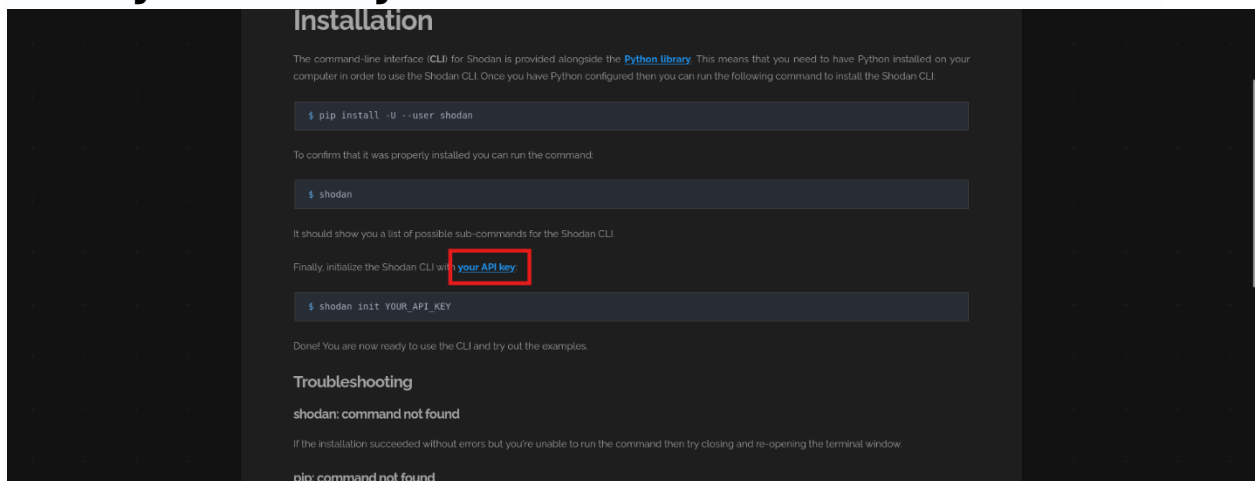
Options:
  -h, --help  Show this message and exit.

Commands:
  alert      Manage the network alerts for your account
  convert    Convert the given input data file into a different format.
  count      Returns the number of results for a search
  data       Bulk data access to Shodan
  domain     View all available information for a domain
  download   Download search results and save them in a compressed JSON...
  honeypot   Check whether the IP is a honeypot or not.
  host       View all available information for an IP address
  info       Shows general information about your account
  init       Initialize the Shodan command-line
  myip       Print your external IP address
  org        Manage your organization's access to Shodan
  parse      Extract information out of compressed JSON files.
  radar      Real-Time Map of some results as Shodan finds them.
  scan       Scan an IP/ netblock using Shodan.
  search     Search the Shodan database
  stats      Provide summary information about a search query
  stream     Stream data in real-time.
  trends     Search Shodan historical database
  version    Print version of this tool.
```

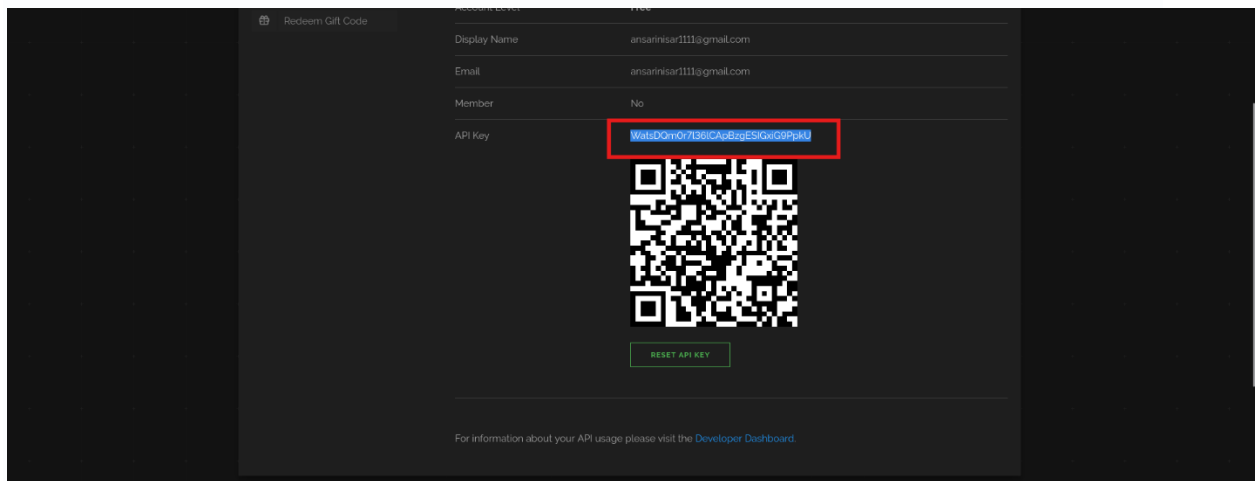
5. Now go back to the shodan developer page and click in the **Get Started** button.



6. Now you have to download the API key by click on the **your API key** button.



7. Now copy your API key.



8. Now go back to the terminal and initialize the API key.

```
(root@kali)-[/home/kali]
# shodan init WatsDQm0r7l36lCApBzgESIGxiG9PpkU
Successfully initialized
```

Shodan CLI Commands:

1. **Domain:** It is used to show the sub domain of the target website.

```
(root@kali)-[/home/kali]
# shodan domain yahoo.com
YAHOO.COM
file.svcn
A 74.6.143.25
A 74.6.143.26
A 74.6.231.20
A 74.6.231.21
A 98.137.11.163
A 98.137.11.164
10000392.ostk.bm2.prod.ir2 A 46.228.36.148
2088221.ostk.bm2.prod.ne1 A 216.155.202.21
628955e1.ostk.bm1.prod.ne1 A 98.137.85.225
714253.ostk.bm2.prod.ne1 A 98.138.48.169
a-looker.eds.vip.corp.gq1 A 67.195.65.106
a1.f62.ymdb.ne1 A 98.138.82.171
a1.in A 203.199.70.9
a135.f96.ymdb.ne1 A 98.138.243.89
a156.f96.ymdb.ne1 A 98.138.243.110
a177.f96.ymdb.ne1 A 98.138.243.131
a18 A 204.71.202.155
a18.f10.ymdb.gq1 A 98.139.112.79
a2.dns.bry A 200.152.165.177
a21.f62.ymdb.ne1 A 98.138.82.175
a32.f62.ymdb.ne1 A 98.138.83.71
a36.f62.ymdb.ne1 A 98.138.83.75
a5 A 204.71.200.45
a5.f91.ymdb.ne1 A 98.138.94.55
a7.f62.ymdb.ne1 A 98.138.82.233
```

2. **Count:** This command checks your current API query quota and usage.

```
(root@kali)-[/home/kali]
# shodan count microsoft iis 10.0
3010942
```


3. Host: This command retrieves detailed information about the host with the IP address 8.8.8.8.

```
(root@kali)-[/home/kali]
# shodan host 8.8.8.8
8.8.8.8
Hostnames:      dns.google
City:           Mountain View
Country:        United States
Organization:   Google LLC
Updated:        2024-05-07T07:18:00.242536
Number of open ports: 2

Ports:
  53/tcp
  53/udp
  443/tcp
    | HTTP title: Google Public DNS
    | Cert Issuer: C=US, CN=WR2, O=Google Trust Services
    | Cert Subject: CN=dns.google
    | SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2, TLSv1.3
```