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

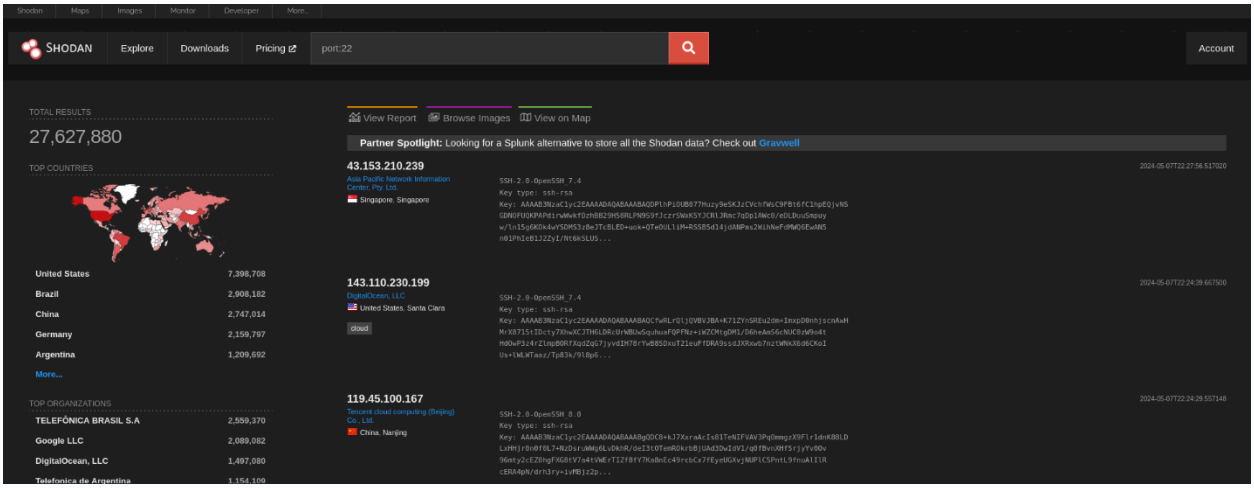
Basically, Shodan tracks public access devices, preferably in SCADA systems (Supervisory Control and Data Acquisition). SCADA systems are used to control and supervise industrial processes remotely in real time.

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.

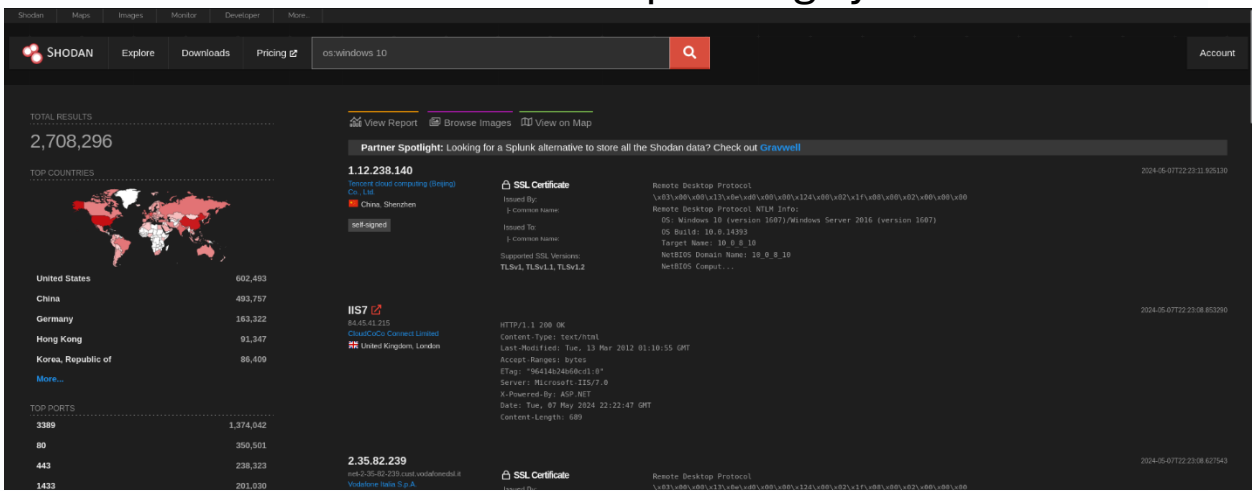
Shodan Web Interface: Shodan's web interface is a search engine for internet-connected devices, offering insights into their vulnerabilities and configurations. Users can search by criteria like location, device type, and software, accessing data on open ports, services, and potential security risks,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

Shodan Web Queries:

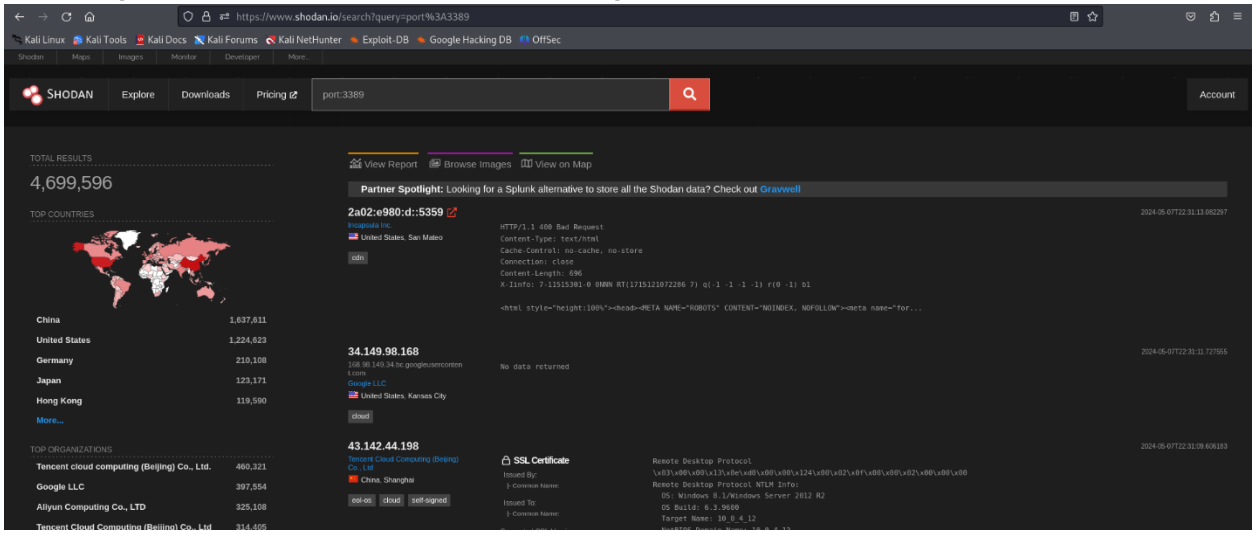
1. **Port:** Port keyword is used to scan for the ports. Here I used port 22 to watch SSH ports.



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

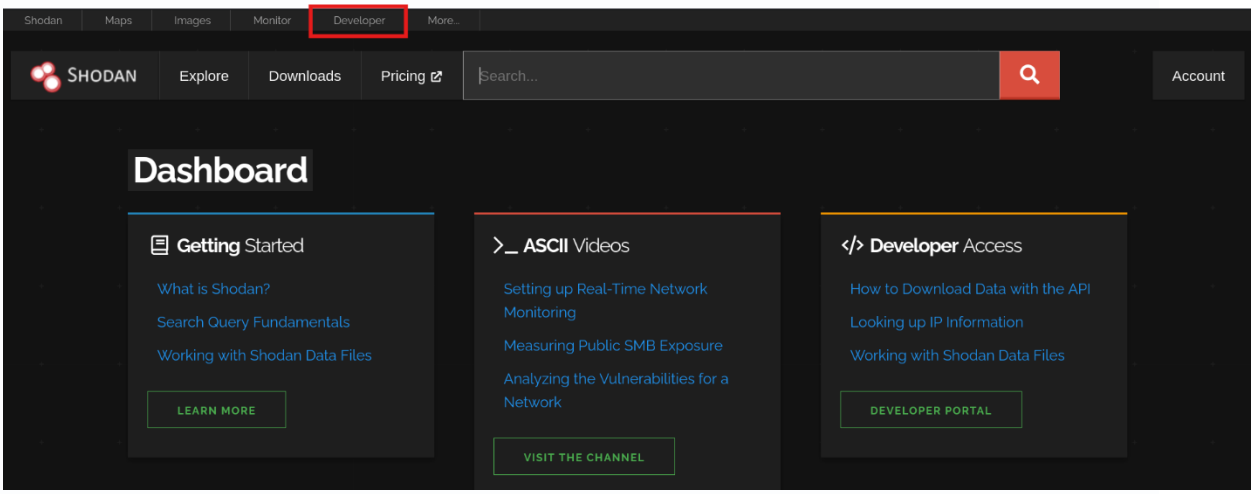


3. **Port:** Port keyword is used to scan for the ports. Here I used port 3389 to watch RDP ports.

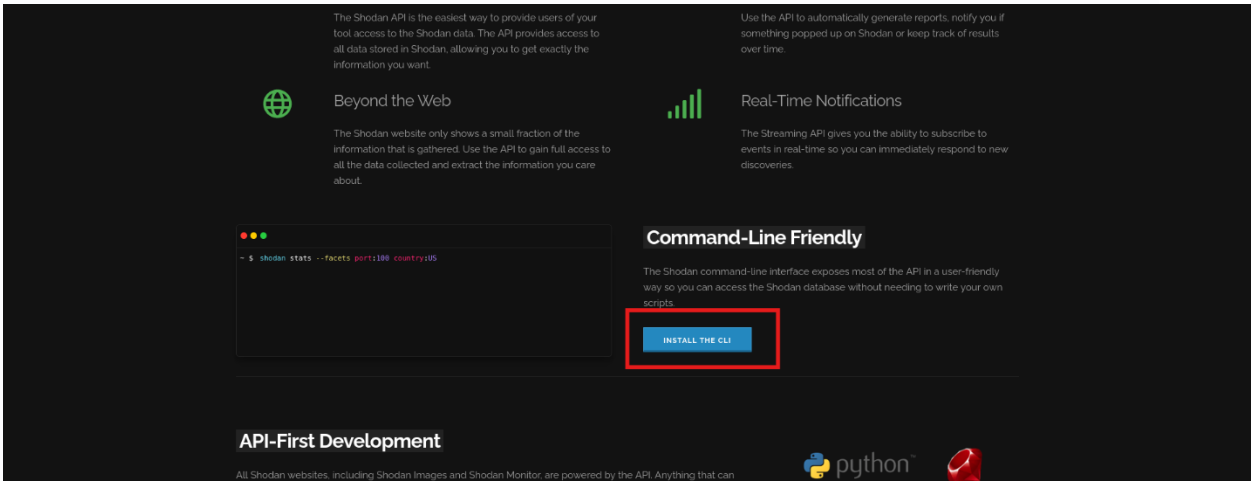


Shodan CLI Downloading steps:

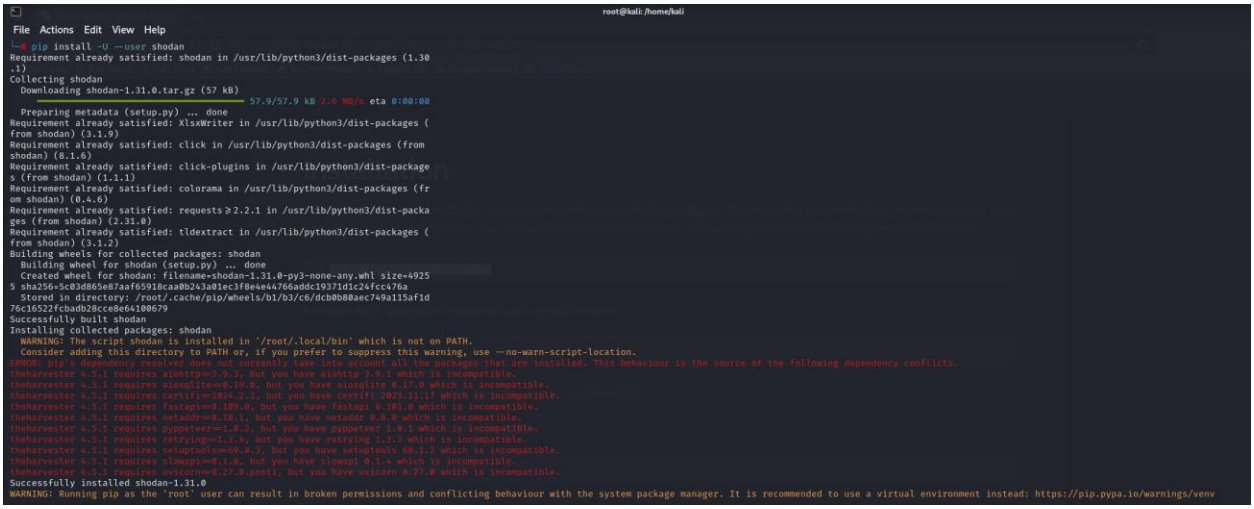
1. Firstly, go to Shodan Dashboard and click on **Developer** option from the task bar.



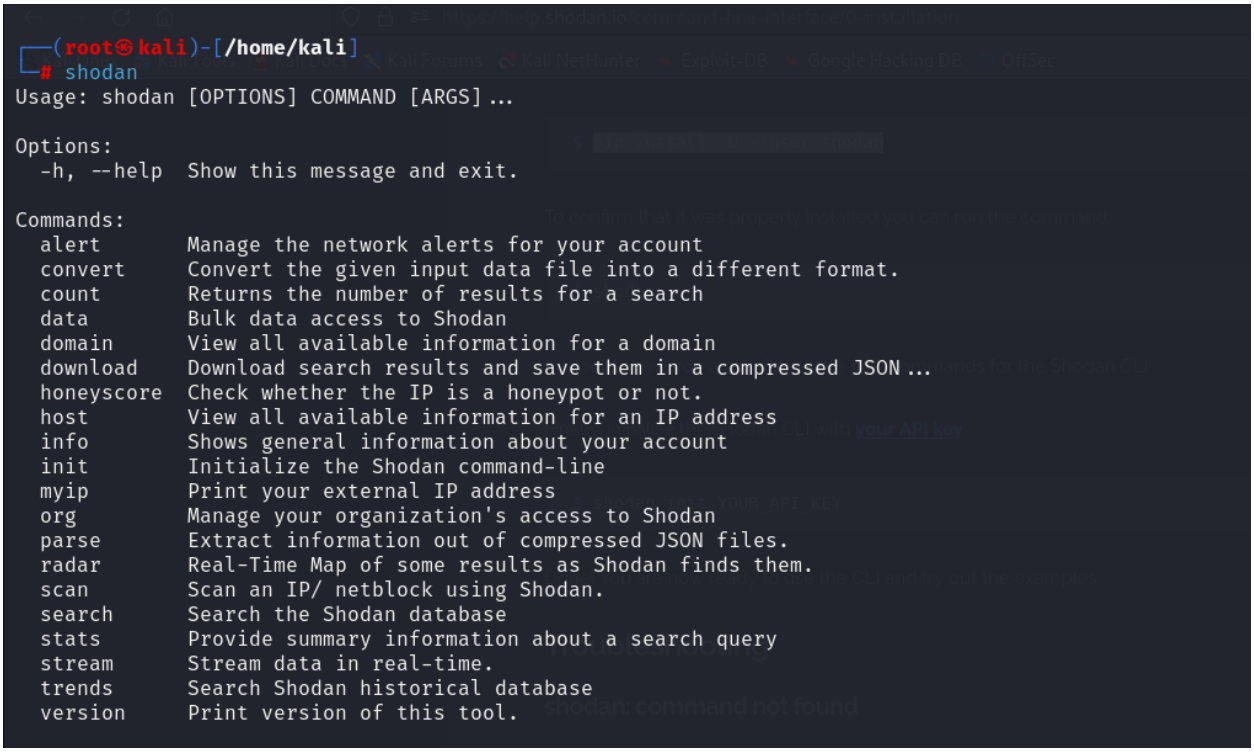
2. Now click on the **Install The CLI** Button.



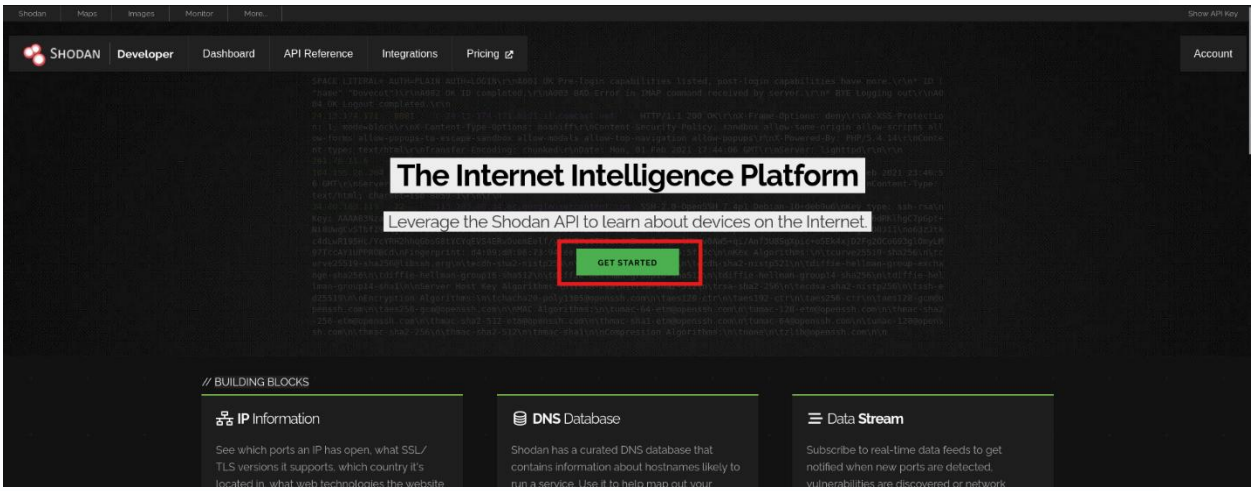
3. Now go to terminal and run the first command.



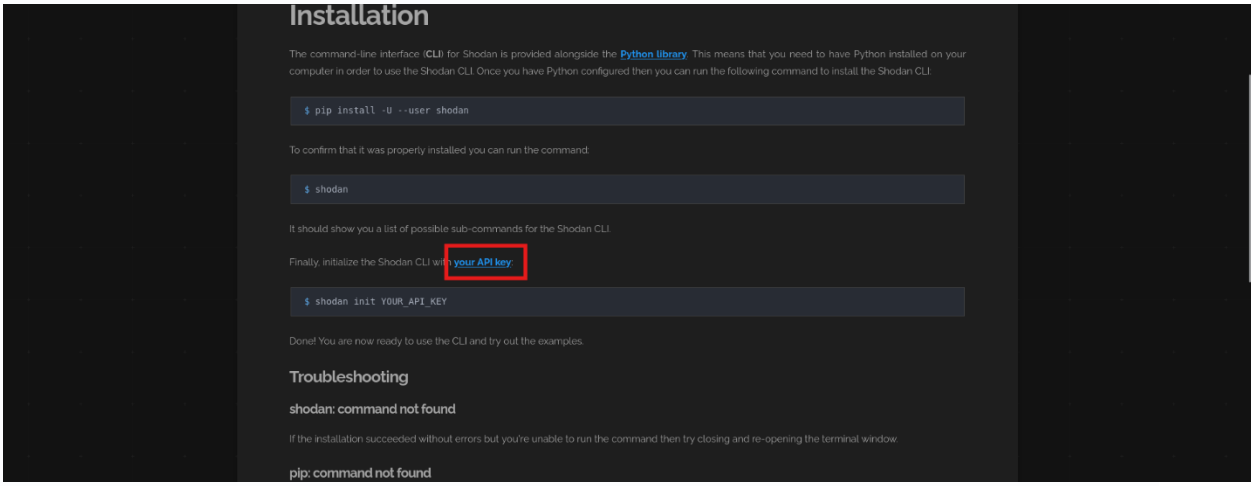
4. Now shodan is installed into your system.



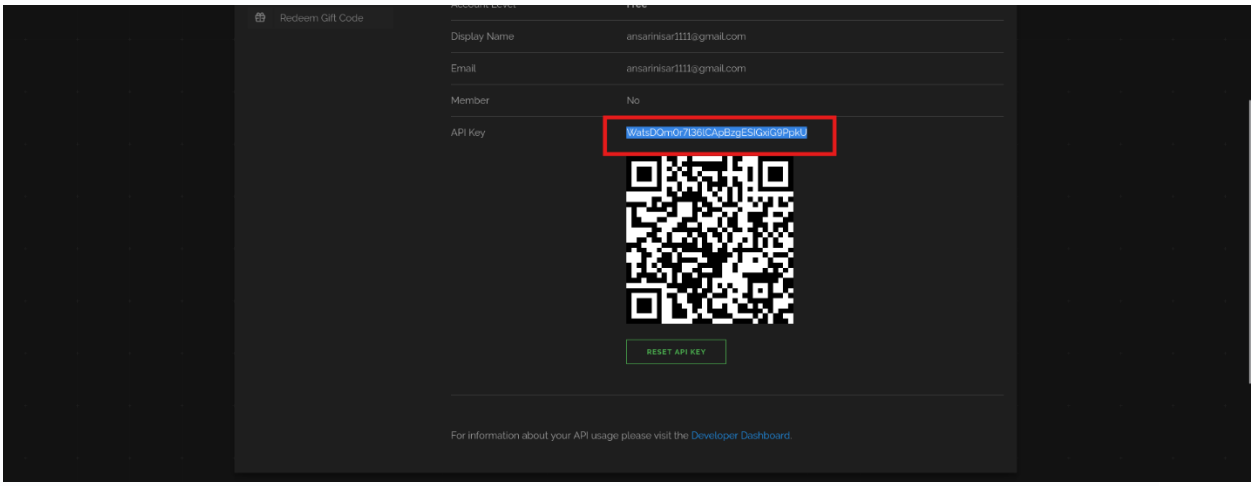
5. Now go back to the shodan developer page and click in the **Get Started** button.



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



7. Now copy your API key.

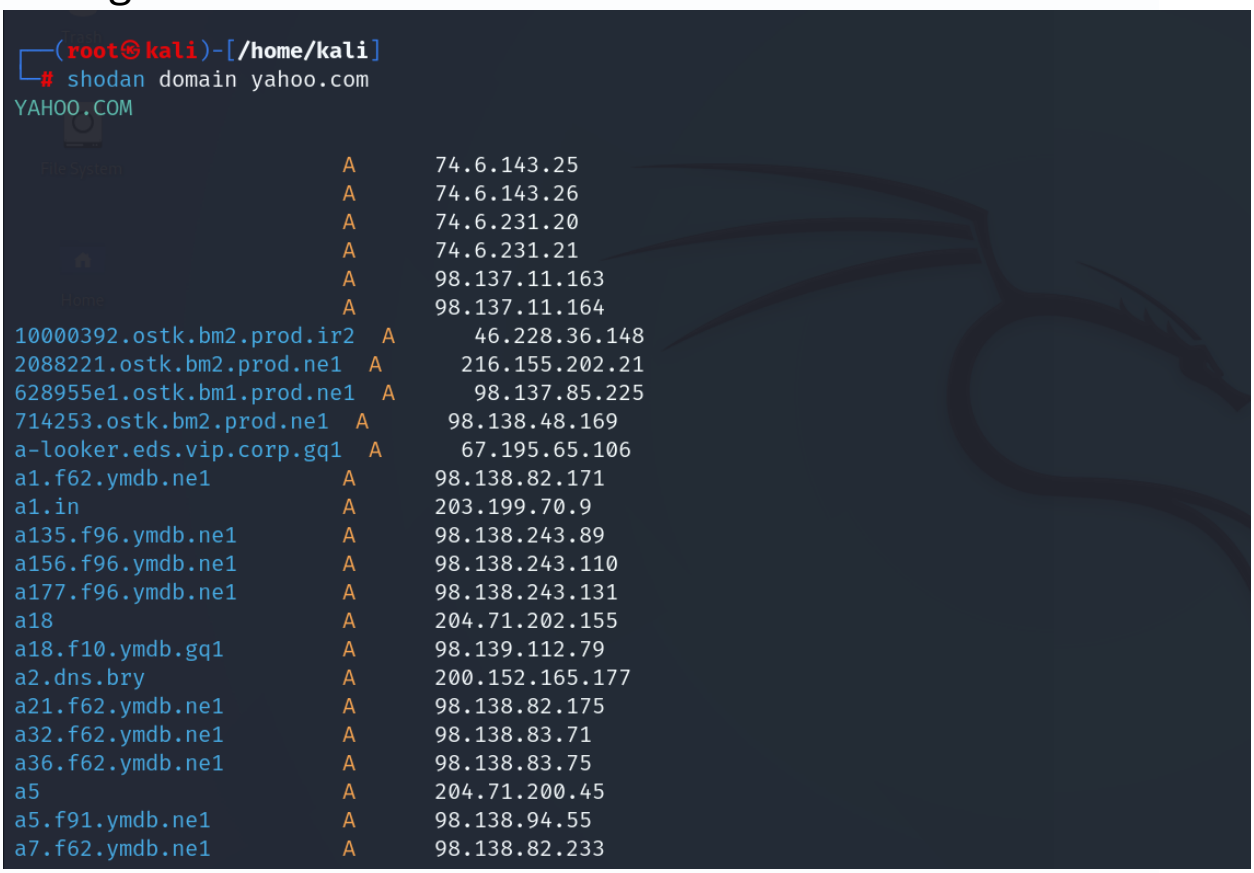


8. Now go back to the terminal and initialize the API key.

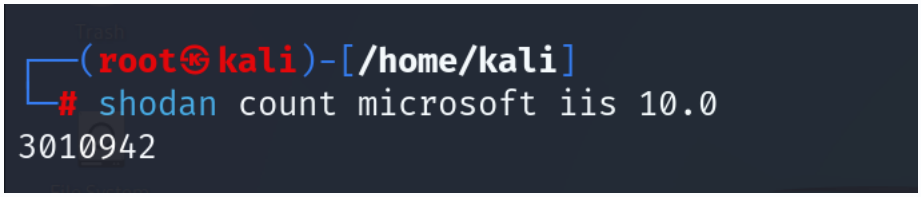
```
┌──(root㉿kali)-[/home/kali]
└─# shodan init WatsDQm0r7l36lCApBzgESIGxiG9PpkU
Successfully initialized
```

Shodan CLI Commands:

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



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



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