

## Lab - Shodan Searches

# Objectives

Shodan is a search engine for IoT devices that was developed by John Matherly in 2009. Shodan can discover all types of internet-connected “things”, from mobile phones to smart appliances, to power plants. It is a powerful tool to determine what devices are currently connected to the network and how they are connected.

- Create a Shodan user account and register for an API key
- Use the Shodan website to search for vulnerable IoT devices
- Use Shodan from the CLI to perform a search

# Background / Scenario

IoT devices are in wide usage. They are created, installed, and maintained by governments, businesses, and homeowners. These devices are not usually hardened by the manufacturer. It is the responsibility of the end-user to ensure that these devices do not introduce additional risks to network security.

You can perform some Shodan searches without obtaining a subscription. More extensive searches require a paid subscription.

In this lab, you will conduct a Shodan search for vulnerable devices within your private network, as well as within a defined IP address range. As with most tools that you are using in this course, only scan or access networks that you own or have permission to access.

# Required Resources

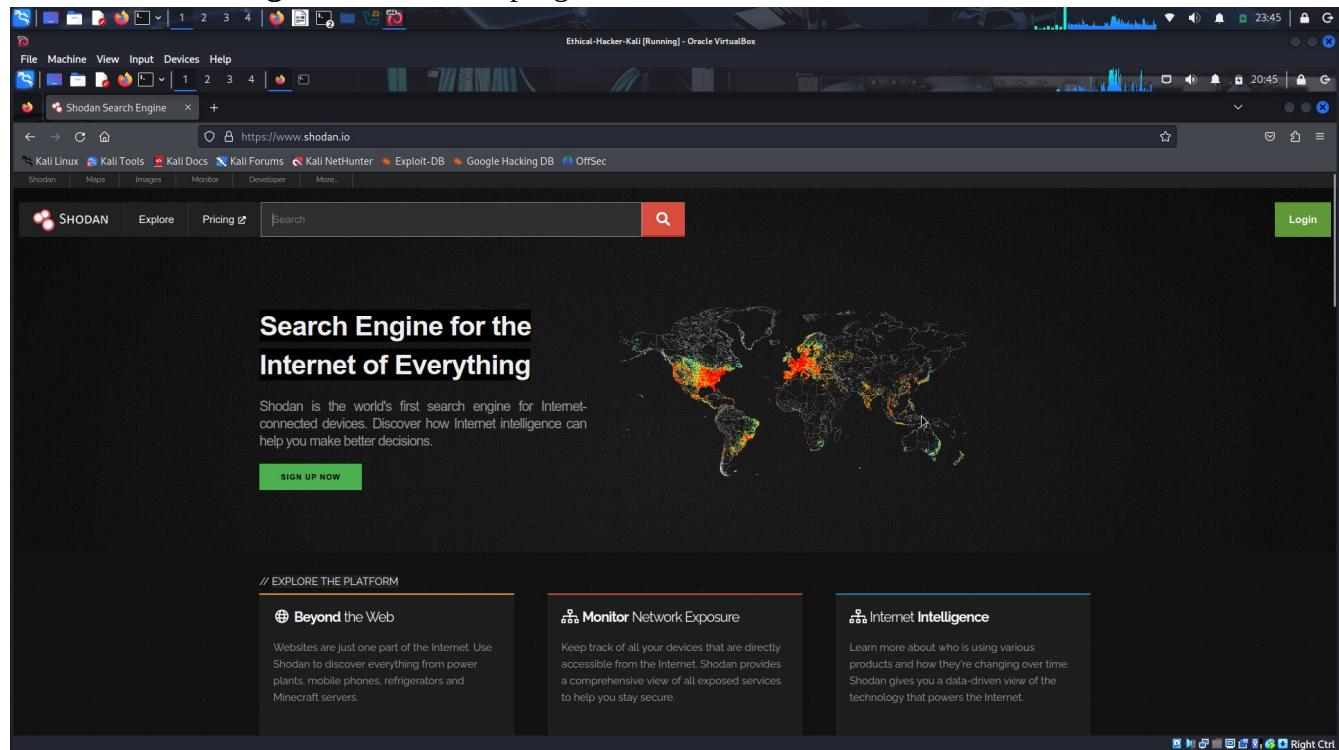
- Kali VM customized for Ethical Hacker course
- Internet access

# Instructions

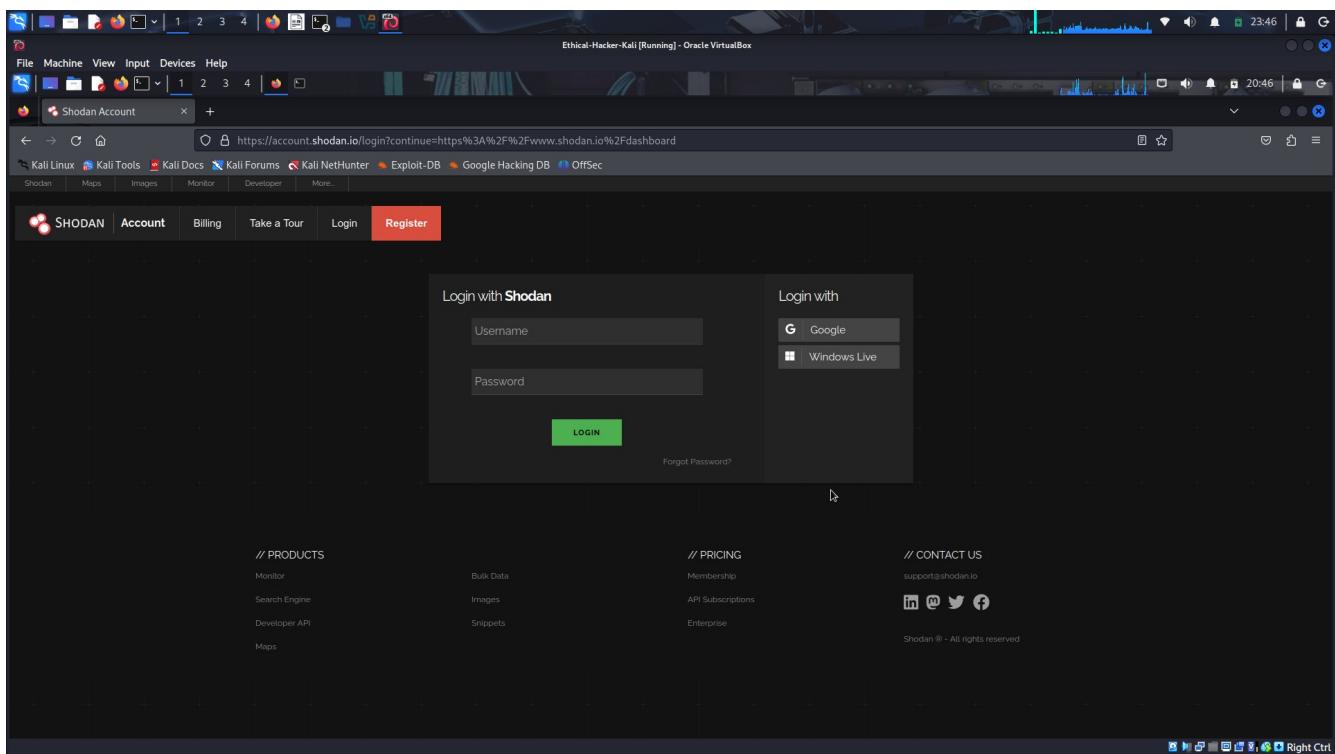
## Part 1: Create a Shodan Account and Register for an API Key

### Step 1: Register for a Shodan account.

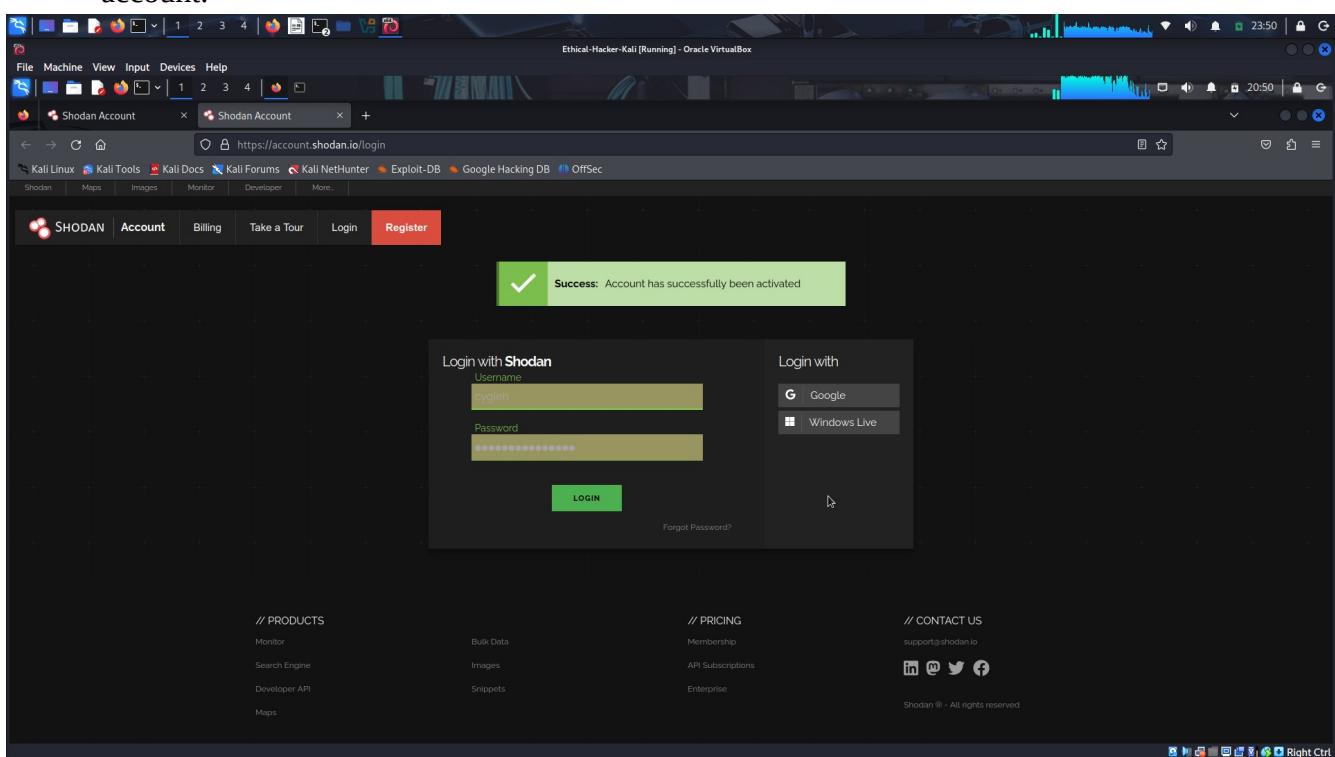
- a. Login to your Kali Linux VM.
- b. Open the Firefox browser and navigate to <https://www.shodan.io/>.
- c. Click the **Login** button at the top right.



- d. On the next screen, click the **Register** button on the menu bar.

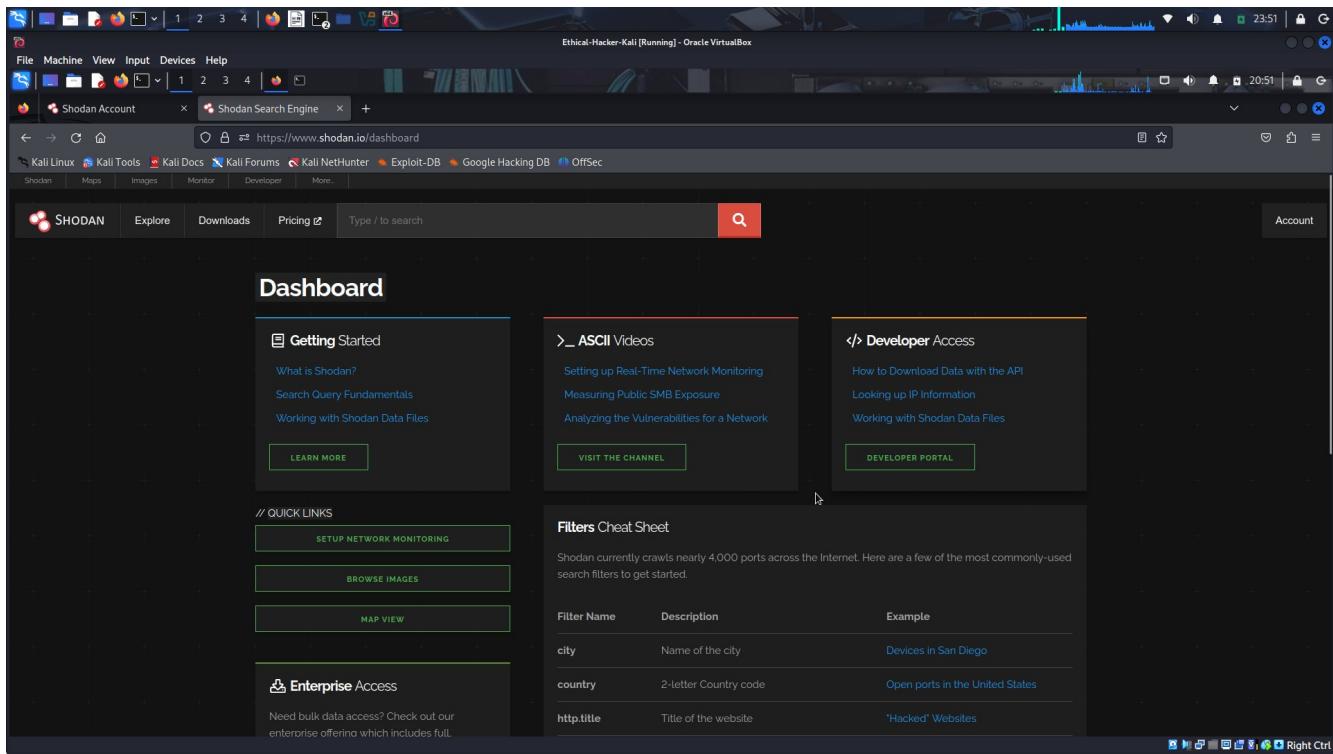


- e. Fill in your information to create a Shodan account. You will receive an email to activate your account.



- f. When your registration is complete, log in to your Shodan account. This is a free account that has several restrictions, including the number of results that will be displayed from each search.

Log in and go to the Shodan home page. Review the **Getting Started** section, especially the **Search Query Fundamentals** link.



## Part 2: Use the Shodan Website to Search for Vulnerable IoT Devices

### Step 1: Use the Shodan search bar to discover IoT devices.

- a. On the Shodan home page, enter **webcam** in the search bar near the top of the screen and press enter.
- b. A page displaying search results will appear. On the left side of the screen are summary statistics. The statistics show the total number of device banners that include the term "webcam", the top countries where the results were found, the top organizations, top products, and top operating systems. You can view up to 10 results without a Shodan login. Registered users can access 50 results for free. Additional services are available with a paid subscription

What is the top country listed with web cams found by Shodan? **USA**

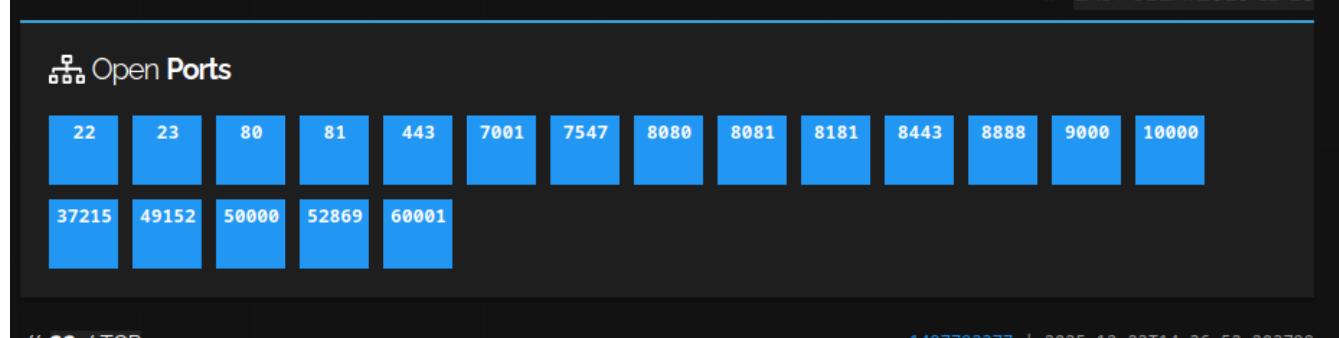
The screenshot shows the Shodan search interface with the query "webcam". The results page displays a world map with red dots indicating device locations. Below the map, there are two sections: "TOP COUNTRIES" and "TOP PORTS". The "TOP COUNTRIES" section lists the United States (812), China (316), Germany (247), United Kingdom (188), and Japan (142). The "TOP PORTS" section lists port 8081 (254), 8080 (169), 443 (93), 80 (76), and 9000 (52). On the right side, several search results are listed with their IP addresses, locations, and dates. For example, one result for "RouterOS router configuration page" from the United States, Atlanta, at 170.187.154.212, was last seen on December 23, 2025, at 18:32:04 GMT.

Click one of the IP addresses listed in the search results. A page with more detailed information opens. At the top of the page, there is a map that shows the approximate location of the search result that you selected. Explore the information for several of the device that were discovered. What information is contained in the General Information section?

The screenshot shows the Shodan device details page for the IP address 163.172.152.168. The page includes a map of Paris and surrounding areas. On the left, there is a "General Information" sidebar with fields for Hostnames (168-152-172-163.instances.scw.cloud), Domains (scw.cloud), Country (France), City (Paris), Organization (SCALEWAY Dedibox - Paris, France), ISP (SCALEWAY S.A.S.), and ASN (AS12876). On the right, there is a "Open Ports" section showing a grid of 16 ports (22, 23, 80, 81, 443, 7001, 7547, 8080, 8081, 8181, 8443, 8888, 9000, 10000, 37215, 49152, 50000, 52869, 60001) in blue boxes. Below the ports, there is a section for "OpenSSH 7.6p1 Ubuntu/4ubuntu0.3" with a long key fingerprint and algorithm details.

On the right side of the output is a list of open ports that Shodan found on the device.

What ports are open on the IP address that you selected?



What information is available for the open ports?

```
// 22 / TCP - 1497793377 | 2025-12-23T14:36:52.203798

OpenSSH 7.6p1 Ubuntu 4ubuntu0.3

SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAQABAAQDda2mL6Mk6T4pPWJRRax/a56tCaTRSx52dxjYVHNMP2QEy
a8ee1sZ3h7TnB5D6ksixkaansT46c40Yu1N5dZpowV3k2MqR/3GWDcrVfwgFI2Cs+0BhZcII/qv
dozu00CcY6xv3KESYkImcP40ICb0EuWygmhW+i29MveyZ24VII3kwpoB25f1XjJYiTaVRqMFdV
1bpnLqhWYNcT7rmZDXRbnz1UyaWs+fbz/N2MwoeC0Z6dq0R1wcMwgVwfHfy0+E34gqBf+EPGEKho
qznKGsJwYyG59/y+zQ5YBcoau71Ads76z0CP0RzRG9xeRidwNOhcedXUtSHFLKxxFF4h
Fingerprint: 1b:9e:3d:05:57:54:de:8f:27:a2:84:a4:9f:92:14:c9

Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group14-sha1

Server Host Key Algorithms:
ssh-rsa
ssh-dss

Encryption Algorithms:
aes128-ctr
aes192-ctr
aes256-ctr
aes256-cbc
aes192-cbc
aes128-cbc
3des-cbc
blowfish-cbc
cast128-cbc

MAC Algorithms:
hmac-sha2-512
```

**Note:** Not all the devices discovered are actually webcams. They are devices that have the word “webcam” somewhere in their service banners.

- e. Search the web for “vulnerable webcam manufacturers.” Frequently, device banners will name the manufacturer of the device.

Some of the devices looked at in the research include the following:

- AXIS net cameras.
- Cisco Linksys webcam.
- IP Camera Logo Server.
- IP WebCam.
- IQ Invision web camera.
- Mega-Pixel IP Camera.
- Mobotix.
- WebCamXP 5.

Vipengee zaidi... • 24 Sep 2019

**Malwarebytes**  
https://www.malwarebytes.com / blog / news / 2019/09 / 15000 webcams vulnerable to attack - Malwarebytes

**Praos Smart Security**  
https://www.praosolutions.com / ... / Taisiri ukurasa huu / List of Security Camera Brands that Have Been Hacked

16 Feb 2024 — Unsecured Cameras: A Notable Concern Axis · Panasonic · PanasonicHD · Linksys · Mobotix · Sony · TP-Link · Foscam ...

**Bitdefender**  
https://www.bitdefender.com / labs / Taisiri ukurasa huu / Vulnerabilities Identified in Wyze Cam IoT Device

Try searching on some manufacturer names in Shodan. From the results, you can refine your search results, sometimes with specific manufacturer's model numbers.

TOTAL RESULTS  
1,130

TOP COUNTRIES

Country	Count
China	122
Brazil	103
Singapore	99
Australia	98
Japan	78
More...	

TOP PORTS

Port	Count
10000	81
1900	44
2083	14
4444	14
443	13
More...	

**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

**103.215.216.105**

free.ds  
G-Core Labs Customer assignment  
India, Andhra Pradesh  
honeypot

HTTP/1.1 200 OK  
Server: MiniUPnPd/1.4  
Pragma: no-cache  
Cache-Control: no-cache  
Content-Type: text/html; charset=utf-8  
Content-Length: 55868

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/tr/xhtml1/DTD/xhtml1-Transitional.dtd">  
<html xmlns="http://www.w3.org/1999...

**5.188.34.165**

example.com  
G-Core Labs Customer assignment  
Singapore, Singapore  
honeypot

HTTP/1.1 200 OK  
Server: MiniUPnPd/1.4  
Pragma: no-cache  
Cache-Control: no-cache  
Content-Type: text/html; charset=utf-8  
Content-Length: 55868

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/tr/xhtml1/DTD/xhtml1-Transitional.dtd">  
<html xmlns="http://www.w3.org/1999...

**TOTAL RESULTS**  
47,875

**TOP COUNTRIES**

Country	Count
Germany	9,817
United States	6,896
Italy	3,470
Spain	3,461
China	2,812
More...	

**TOP PORTS**

Port	Count
80	2,923
443	1,691
9501	1,427
81	1,372
8001	1,111
More...	

**Error 401: Unauthorized access**

```

HTTP/1.1 401 Unauthorized
Server: mxhttpd/2.19-MK Mar 14 2017
Content-type: text/html
Date: Wed, 17 Dec 2025 16:03:24 GMT
Last-modified: Wed, 17 Dec 2025 16:03:24 GMT
Accept-Ranges: bytes
Connection: close
Content-length: 7463
WWW-Authenticate: Basic realm="MOBOTIX Camera User"
WWW-Authe...

```

**Error 401: Unauthorized access**

```

HTTP/1.1 401 Unauthorized
Server: mxhttpd/2.19-MK Oct 24 2018
Content-type: text/html
Date: Tue, 23 Dec 2025 17:06:53 GMT
Last-modified: Tue, 23 Dec 2025 17:06:53 GMT
Accept-Ranges: bytes
Connection: close
Content-length: 7463
WWW-Authenticate: Basic realm="MOBOTIX Camera User"
WWW-Authe...

```

**Error 401: Unauthorized access**

```

HTTP/1.1 401 Unauthorized
Server: mxhttpd/2.19-MK Jan 28 2020
Content-type: text/html
Date: Fri, 23 Dec 2025 17:06:53 GMT
Last-modified: Fri, 23 Dec 2025 17:06:53 GMT
Accept-Ranges: bytes
Connection: close
Content-length: 7463
WWW-Authenticate: Basic realm="MOBOTIX Camera User"
WWW-Authe...

```

In addition, search for default logins used by camera model. It is possible that the owner of camera did not change the default password.

**default logins used by camera model**

**Manufacturer List Default Passwords**

- ACTi: admin/123456 or Admin/123456.
- **Amcrest**: admin/admin.
- American Dynamics: admin/admin or admin/9999.
- Arecont Vision: none.
- AvertX: admin/1234.
- Avigilon: Previously admin/admin, changed to Administrator/<blank> in later firmware versions.

Vipenge zaide... • 9 Feb 2018

**IPVM**  
https://ipvm.com/reports/ip-cameras-default-passwords/

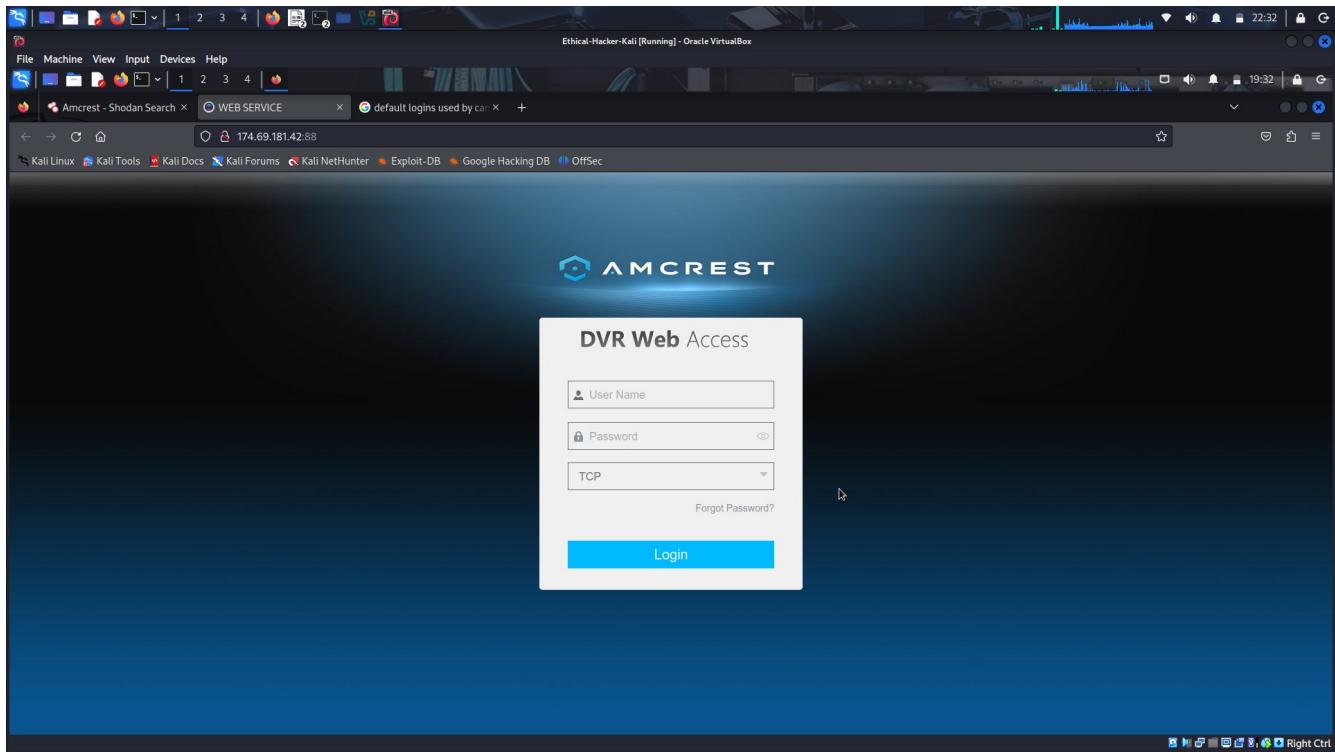
**IP Cameras Default Passwords Directory - IPVM**

**A1 Security Cameras**  
https://www.a1securitycameras.com/... - Tässä sivulla löytyy kaikki A1 Security Camera -tuotemerkkiset kameroita ja niiden käytössä olevat käyttäjätunnukset ja salasanat.

**Default Username - Password - IP Address for...**  
25 Jan 2023 — Surveillance Brands - Default Username and Passwords ; Messoa, admin, Model# of camera, 192.168.1.30 ; Mobotix, admin, meinism, No Default / DHCP.

**General: Default Camera Passwords**  
This is a list of the default login credentials (usernames, passwords and IP addresses) for logging into...

**DO NOT** attempt to login to devices that you do not own or have permission to access.



## Step 2: Use Shodan filters to refine the results.

Shodan provides a method to filter your search results using the syntax ***filter:value*** with no spaces. If the value contains spaces, such as **city:"los angeles"**, you must enclose the value in double quotes. Some of the most popular search filters are:

**country:XX** Searches for a 2 digit country code

**city:city-name** Searches for a city by name

**region:region-or-state-name** Searches for a specific state or region

**product:product-name** Searches for a specific product by name

**version:XX** Searches for a specific product version

**vuln:XX** Searches for vulnerabilities that match a specific CVE number

- Enter a filter on the Shodan search bar. This example returns all the devices with “webcam” in a banner that Shodan finds in the city of Toronto.

**webcam city:Toronto**

TOTAL RESULTS  
39

TOP PORTS

PORT	COUNT
8081	3
80	2
81	2
443	2
7001	2
More...	

TOP ORGANIZATIONS

ORGANIZATION	COUNT
Linode	19
Linode, LLC	18
Rogers Communications Canada Inc.	1
The North Frontenac Telephone Corporation Limited	1

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

View Report | View on Map | Advanced Search

192.53.123.104 [ ]  
 192.53.123.104.ip.linodeusercontent.com  
 Linode, LLC  
 Canada, Toronto  
 cloud honeypot

192.53.123.104 [ ]  
 192.53.123.104.ip.linodeusercontent.com  
 Linode, LLC  
 Canada, Toronto  
 cloud honeypot

192.53.123.104 [ ]  
 192.53.123.104.ip.linodeusercontent.com  
 Linode, LLC  
 Canada, Toronto  
 cloud honeypot

192.53.123.104 [ ]  
 192.53.123.104.ip.linodeusercontent.com  
 Linode, LLC  
 Canada, Toronto  
 cloud honeypot

2025-12-23T18:27:11.07436  
 2025-12-23T18:19:17.07667  
 2025-12-23T18:16:20.75395  
 2025-12-23T17:46:47.03766

- b. A common configuration issue found on the internet is FTP servers that permit anonymous logins. Use the search string to find the FTP servers in San Jose, California.

**port:21 country:US region:CA city:"San Jose" 230**

TOTAL RESULTS  
452

TOP ORGANIZATIONS

ORGANIZATION	COUNT
Verizon Business	71
GTT	63
Microsoft Corporation	26
Alibaba Cloud - US	22
BigBiz Internet Services	14
More...	

TOP PRODUCTS

PRODUCT	COUNT
Pure-FTPd	101
Microsoft ftpd	30
WU-FTPD	9
ProFTPD	6
FreeBSD ftpd	5
More...	

TOP OPERATING SYSTEMS

OPERATING SYSTEM	COUNT
Windows	33
Unix	20
More...	

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to](#).

173.228.19.69  
 piddu.com  
 Systech, Inc  
 United States, San Jose

220 Welcome to Piddu FTP. Kindness is never wasted.  
 230 Login successful.  
 214- The following commands are recognized.  
 ABLR ACCT ALLO APPE CWD DELE EPRT EPSV FEAT HELP LIST MOTH MKD  
 MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR  
 RNT SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCP XCMD XCWD...

71.19.145.72  
 facemind.wu.org.com  
 pggc.com, Inc  
 United States, San Jose

220 (w)FTPd 3.0.3)  
 230 Login successful.  
 214- The following commands are recognized.  
 ABLR ACCT ALLO APPE CWD DELE EPRT EPSV FEAT HELP LIST MOTH MKD  
 MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR  
 RNT SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCP XCMD XCWD...

192.19.158.87  
 bsrnupport-stage-internal broadband-downloads-01b9-0prod.broadcom.com  
 bsrnupport-stage-internal broadband-downloads-01b9-0prod.broadcom.com.net  
 bsrnupport-tp-gprod-internal broadband-downloads-01b9-0prod.broadcom.com.net  
 support@broadcom.com  
 Apple Inc, Cupertino, U.S. Inc  
 United States, San Jose  
 starlits

SSL Certificate  
 Issued By: 220-Broadcom Managed File Transfer - DMZ - (w)FTP83  
 Common Name: 220-Broadcom Managed File Transfer Server Ready!  
 230- Password OK Connected  
 214- The following commands are recognized (\*-->'s unimplemented).  
 214-USER PORT STORE MSAM\* BNTO NLST MKD CGUP  
 214-PASS PASV APPE...  
 Issued To: 214-Organization: Broadcom Inc  
 Common Name: download-pprod.broadcom.com  
 Organization: Broadcom Inc

2025-12-23T18:13:25.698365  
 2025-12-23T18:03:45.722364  
 2025-12-23T18:03:45.722364

This search uses the standard FTP TCP port 21, with location filters, and a text search for 230. 230 is the FTP successful login response code.

Shodan searches can identify cloud applications and possible honeypots. Browse the search results from your queries to find results labeled **cloud** or **honeypot**.

The screenshot shows the Shodan search interface with the query "cloud". The results page displays a map of the world with red dots indicating found locations. A sidebar on the left lists "TOP COUNTRIES" with the United States having 121,386 results. On the right, detailed results for three specific IP addresses are shown:

- 34.54.143.97**: Located in the United States, Kansas City. SSL certificate issued by Cloudflare Inc. to Google LLC. The certificate is valid until 2025-12-23T19:37:49Z. The response code is 200 OK.
- 165.140.157.148**: Located in the United States, Dallas. SSL certificate issued by RapidSSL TLS RSA CA G1 to cloud7-eae450.managed-vps.net. The certificate is valid until 2025-12-23T19:37:41Z. The response code is 200 OK.
- 138.43.107.202**: Located in Hungary, Budapest. SSL certificate issued by RapidSSL TLS RSA CA G1 to iobis Inc. The certificate is valid until 2025-12-23T19:37:30Z. The response code is 200 OK.

The screenshot shows the Shodan search interface with the query "honeypot". The results page displays a map of the world with red dots indicating found locations. A sidebar on the left lists "TOP COUNTRIES" with Hungary having 257 results. On the right, detailed results for two specific IP addresses are shown:

- 9.33.175.69**: Located in the United States, Seattle. SSL certificate issued by Amazon Technologies Inc. to Onshape. The certificate is valid until 2025-12-23T18:19:08Z. The response code is 200 OK.
- 91.236.182.139**: Located in Hungary, Budapest. SSL certificate issued by Debian GNU/Linux 11 to Brilliant Auto Kft. The certificate is valid until 2025-12-23T18:15:23Z. The response code is 200 OK.

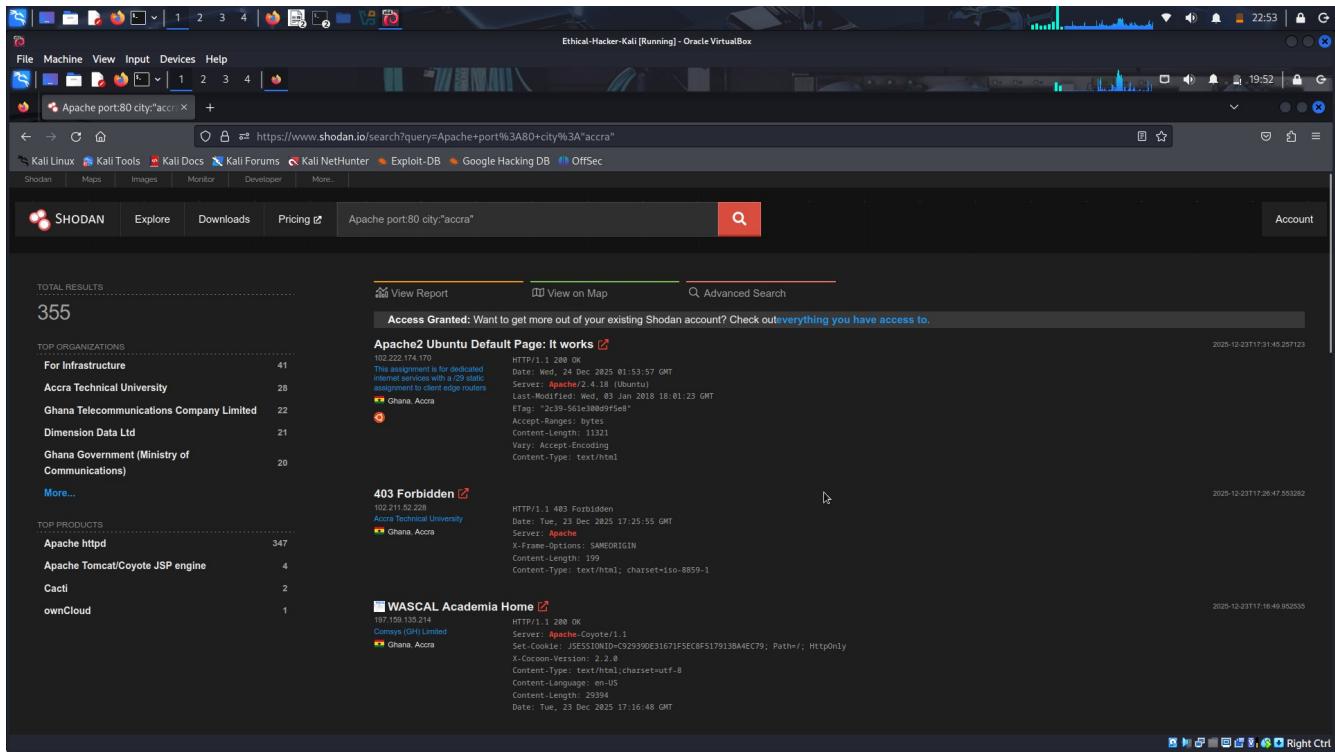
Click one of the results labeled **cloud** to open the details page.

The screenshot shows a Kali Linux desktop environment with a Shodan search result for the IP address 217.16.1.171. The search results are displayed in a browser window titled "Ethical-Hacker-Kali (Running) - Oracle VirtualBox". The Shodan interface includes a map of the area around Vitrolles, France, with various locations labeled. The search results are organized into sections: General Information, Open Ports, and Remote Desktop Protocol. The General Information section lists hostnames (vm1-19.hosteur.net), domains (hosteur.net), country (France), city (Vitrolles), organization (HOSTEUR SAS), ISP (HOSTEUR SAS), ASN (AS204818), and operating system (Windows (build 10.0.17763)). The Open Ports section highlights port 3389 as TCP. The Remote Desktop Protocol section provides detailed information about the connection, including the OS (Windows 10 (version 1809)/Windows Server 2019 (version 1809)), OS Build (10.0.17763), Target Name (CLOUD-568JA030), NetBIOS Domain Name (CLOUD-568JA030), NetBIOS Computer Name (CLOUD-568JA030), DNS Domain Name (cloud-xdobja030), and FQDN (cloud-568ja030). The SSL Certificate section shows a self-signed certificate with version 3 (0x2).

### Step 3: Use Shodan to search for a specific product or service.

You can use Shodan to search for a specific product, such as Apache servers open on port 80. Formulate a query to find the Apache servers in your city.

**Apache port:80 city:"your-city"**

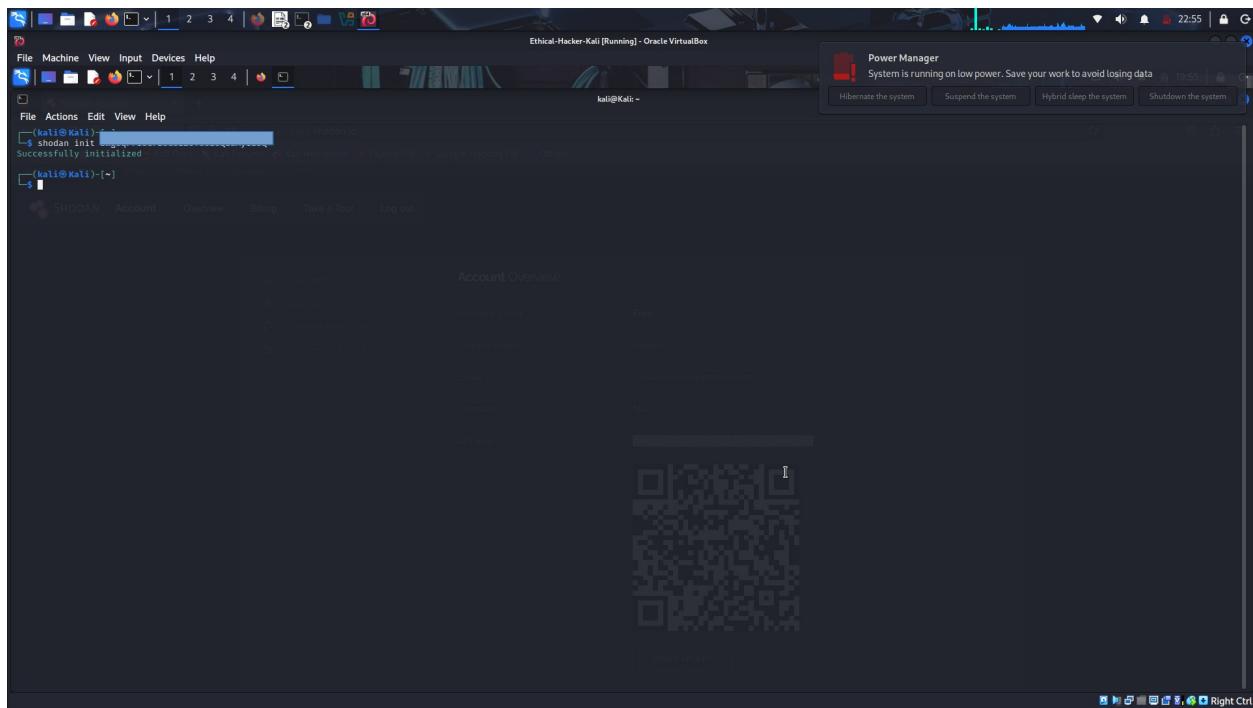


## Part 3: Use Shodan from the CLI to Perform a Search

### Step 1: Initialize Shodan and perform a search.

- Find and copy your API key by selecting **Account > Overview** from the top right of the Shodan web site screen. Highlight the API key shown above the QR code, right-click the selection and select **Copy**. Make note of your key for future use.
- Shodan is a Python library that is installed in Kali by default. Open a Kali terminal window.
- At the prompt, enter the command **shodan init** and right click and select **Paste Selection** to paste the API key into the terminal. Your API key should appear at the end of the command.

This command should return the string “Successfully initialized”.



- d. Enter the **shodan -h** command to display the list of Shodan commands available from the command line.

```
(kali㉿Kali)-[~]
$ shodan -h
Usage: shodan [OPTIONS] COMMAND [ARGS] ...

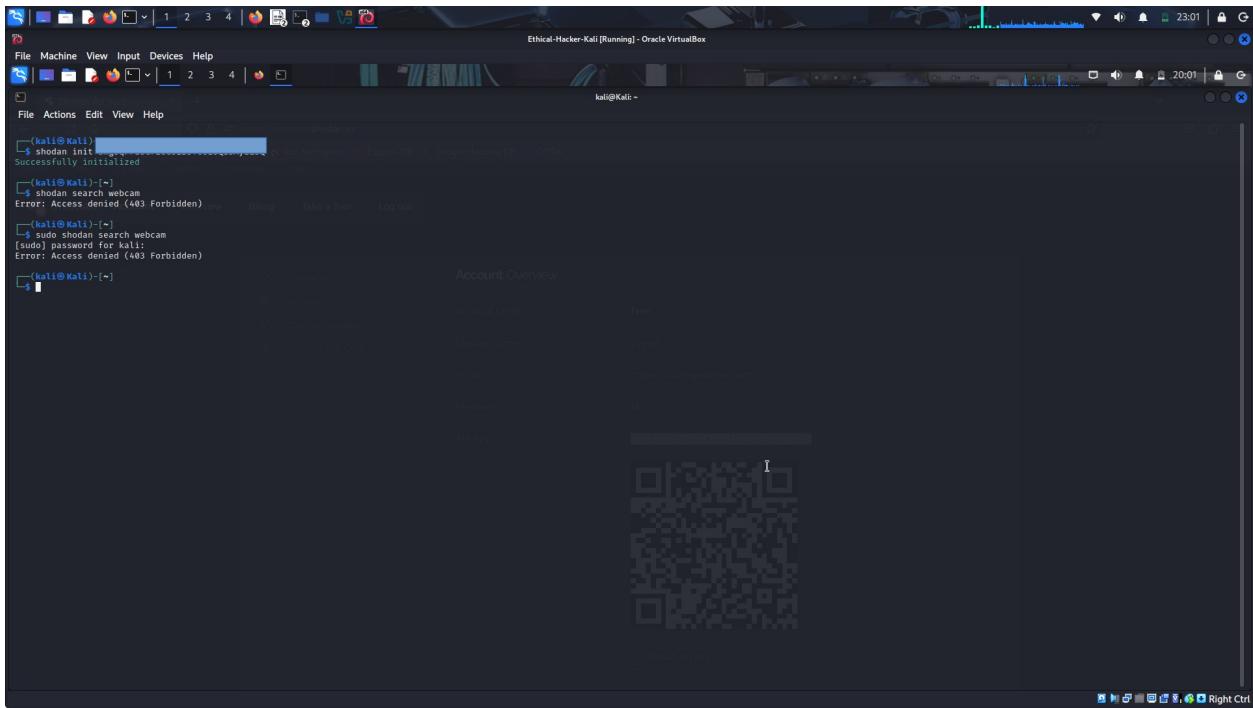
Options:
-h, --help Show this message and exit.

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 ...
honeyscore 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.
version   Print version of this tool.
```

- e. Execute the same search at the CLI that you did in the web search bar to view webcams that Shodan finds. At the CLI, you must enter the **shodan search** command before specifying the search criteria.

The output of the command is unformatted text. The IP addresses of the devices that Shodan finds are highlighted along with the port and the device name. Press **q** to quit and return to the CLI prompt. Shodan CLI commands can be written into Python scripts to automate search and scanning functions.

**Note:** Searching with filters is not available with a free API key.



A screenshot of a Kali Linux terminal window titled "Ethical-Hacker-Kali [Running] - Oracle VirtualBox". The terminal shows the following session:

```
(kali㉿Kali)-[~]
$ shodan init
Successfully initialized

(kali㉿Kali)-[~]
$ shodan search webcam
Error: Access denied (403 Forbidden)

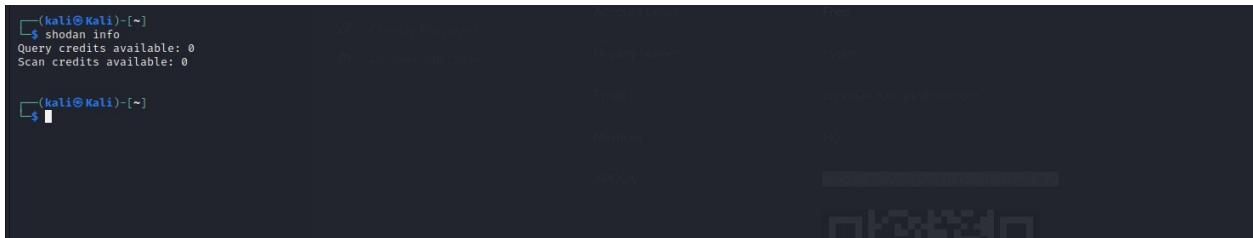
(kali㉿Kali)-[~]
$ sudo shodan search webcam
[sudo] password for kali:
Error: Access denied (403 Forbidden)

(kali㉿Kali)-[~]
```

The terminal window is part of a desktop environment with multiple windows open in the background, including a file manager and a browser.

## Step 2: Execute other Shodan CLI commands.

- Not all commands listed are available in the free version of Shodan. The **shodan info** command will show how many credits that you currently have to perform searches or scans.



A screenshot of a Kali Linux terminal window showing the output of the **shodan info** command:

```
(kali㉿Kali)-[~]
$ shodan info
Query credits available: 0
Scan credits available: 0

(kali㉿Kali)-[~]
```

For paid subscriptions, the available credits will reset each month. There are subscriptions available for a cost that permit unlimited queries and scans.

- Use the **shodan myip** command to find the registered IP address that corresponds to your device.

The IP address returned is the source IP address that will be added to any packets sent from your device to a destination on the internet.

```
[kali㉿Kali)-[~]
└─$ shodan myip
[REDACTED]

[kali㉿Kali)-[~]
└─$
```

- c. Another useful command is the **stats** command. It will return the summary information about a query, similar to what is displayed on the results page in the web version. To get the summary information, enter the stats command and the search query that you want to view the results.

```
[kali㉿Kali)-[~]
└─$ shodan stats webcam
Top 10 Results for Facet: country
US          808
CN          318
DE          246
GB          185
JP          143
SG          115
IT           97
KR           71
KZ           67
CA           65

Top 10 Results for Facet: org
Linode        804
Aliyun Computing Co., LTD    196
Linode, LLC      145
139.162.0.0/16     124
Alibaba Cloud (Singapore) Private Limited 78
Hoster.KZ        67
Deutsche Telekom AG      62
Aliyun Computing Co.LTD    60
Scaleway - Warsaw, Poland 50
Korea Telecom      37

[kali㉿Kali)-[~]
└─$
```

This query returns the summary statistics for the webcam search.