**UNIT-II**

***Chapter IV :- SHODAN***

**What is shodan?**

Shodan (**Sentient Hyper-Optimized Data Access Network**) is a search engine for hackers, and have even called it **“the world’s most dangerous search engine**”. [Shodan](http://www.shodanhq.com/) is used for finding specific devices, and device types, that exist online. It was developed by **John Matherly in 2009**, and unlike other search engines, it looks for specific information that can be invaluable to hackers.

Shodan is a type of search engine that allows users to search for Internet-connected devices and explicit website information such as the type of software running on a particular system and local anonymous FTP servers. Shodan can be used much in the same way as Google, but indexes information based on banner content, which is meta-data that servers send back to hosting clients. For the best results, Shodan searches should be executed using a series of filters in a string format.

**Why scan with shodan?**

1. Shodan is a search engine for finding specific devices, and device types, that exist online.

2. It is like an internet map that lets us see which device is connected to which or ports are open on a specific device or what operating system a certain system is using, etc.

3. Rather than to locate specific content on a particular search term, SHODAN is designed to help the user find specific nodes (desktops, servers, routers, switches, etc.) with specific content in their banners.

**What Shodan can do?**

Shodan pulls **service banners** from servers and devices on the web, mostly **port 80, but also ports 21 (ftp), 22 (SSH), 23 (telnet), 161 (SNMP), and 5060 (SIP).** Since almost every new device now has a web interface (maybe even your refrigerator) to ease remote management, we can access innumerable web-enabled servers, network devices, home security systems, etc.

**How it works?**

It works by scanning the entire Internet and parsing the banners that are returned by various devices. Using that information, Shodan can tell you things like what web server (and version) is most popular, or how many anonymous FTP servers exist in a particular location, and what make and model the device may be.

**What devices can Shodan really find:**

1) Servers

2) Routers

3) Switches

4) Printers on public ip

5) Webcams

6) Gas station pumps

7) Voip phones And all Scada (supervisory control and data acquisition)devices.

**The most popular searches:**

Shodan can find us webcams, traffic signals, video projectors, routers, home heating systems, and SCADA systems that, for instance, control nuclear power plants and electrical grids. If it has a web interface, Shodan can find it! Although many of these systems communicate over port 80 using HTTP, many use telnet or other protocols over other ports.

**Working of Shodan:**

1. User searches for a particular item.
2. Shodan probes for ports and captures the resulting banners.
3. Now, Shodan indexes the captured banners.
4. After indexing,it displays the results.

**Difference between Shodan and google:**

of web content and then displays the results according to the page rank which in turn depends on a number of factors. Shodan mainly looks for ports and then grabs the resulting banners and indexes them. And finally, it displays the results. It does not index web content (the key point) like google and thus it is a search engine of banners.

**Basic filters in Shodan**

shodan has several powerful yet easy to use filters which prove handy during VA/PT exercises. The usage of filters is usually of the form **filter:value**.Some of the most common basic filters that you can use in Shodan are as follows.

**1.** **Country**: The country filter allows users to search for computers running services in a particular country. The country code is specified as a two-letter word.

**Usage**: cisco country: IN (searches for Cisco devices in the particular country. In this case, it’s India).

**2.** **Host name:**This useful option in Shodan lets you find a particular service or the service running in specified hosts or domains.

**Usage:**"Server:IIS" host name: domain name

                         Host name: domain name

**3.** **Net:**This filter is used to scan a particular IP address or subnet range. The service name can also be added along with the IP address or subnet.

**Usage: For scanning an IP address:**net: 198.162.1.1(any IP)

**For scanning a subnet:** net: 198.162.1.1/24

**4.** **Port:**This filter allows you to scan a particular service. For instance, FTP (21), HTTP (80).

**Usage:**Service port number

**Example**: IIS port: 80

**5.** **Operating system (OS):**This Shodan filter helps you to identify a service with a required OS. You can use it to find the service running on the particular OS.

**Usage:**Service: OS: OS name

**Example**: IIS “OS: OSName”

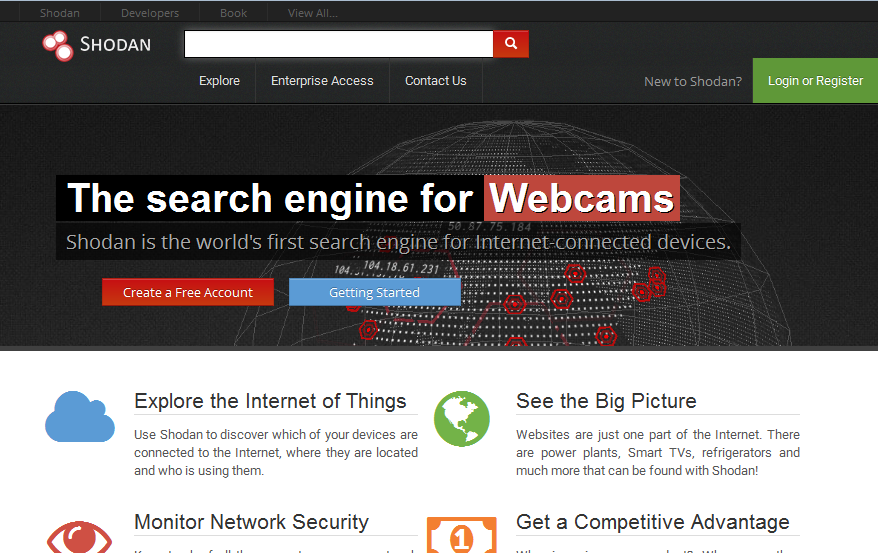
**6.** **After/before:**This option helps or returns the query, changed or unchanged before.

**Example:** apache after: 22/03/2010 before: 4/6/2010

**Example:**apache country: CH after:22/03/2010 before: 4/6/2010

**How to use Shodan?**

Understanding shodan is very important at first you might find it complex but once you get to know it you will find it very handy in use and  very resource full too. So, now let us learn how to work with fascinating search engine. To use shodan to your advantage you have Follow the steps to register.

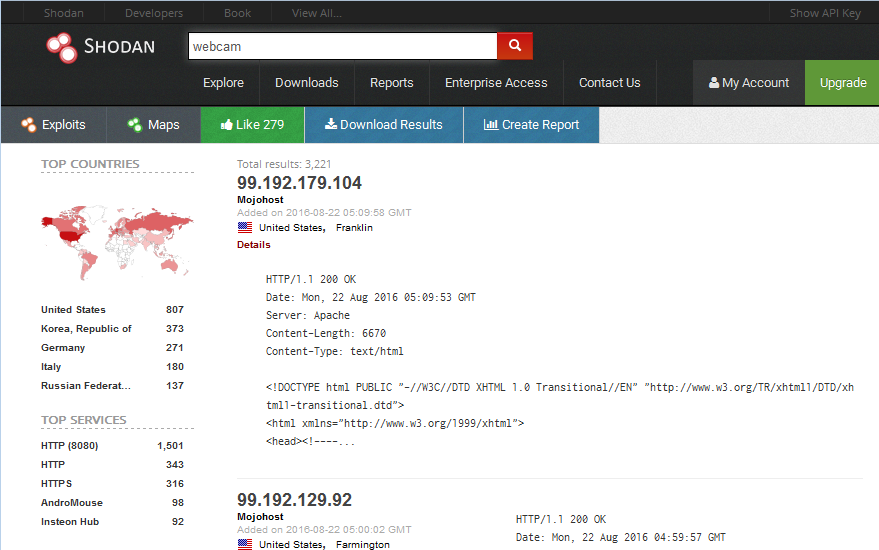


After registration a link will be sent to your e-mail ID for your activation of account on Shodan. Once your account is activated login to Shodan and now that you are logged in you are free to search anything.

Here are some examples for which you can use shodan to search up the things you want.

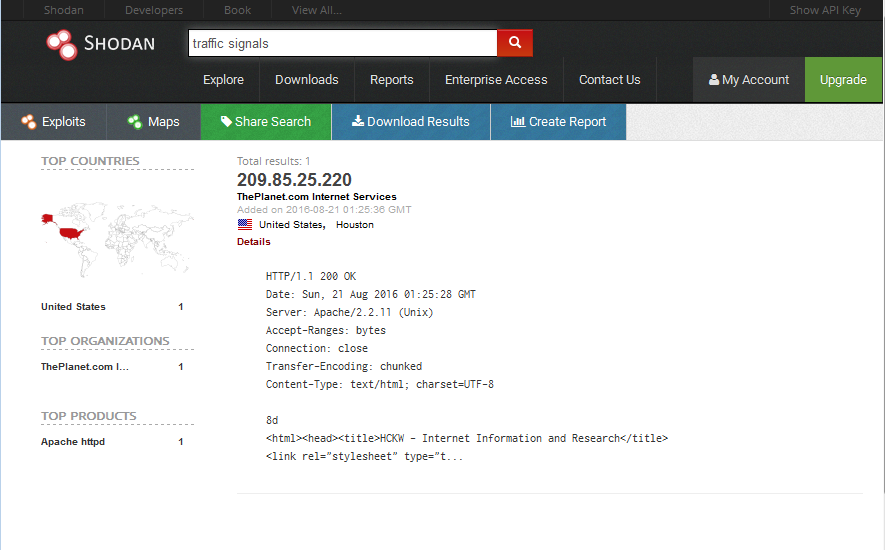
1. **Webcam**

When you search for webcam, it will show you all the webcam present in the world. It will show the results as shown in the image below :



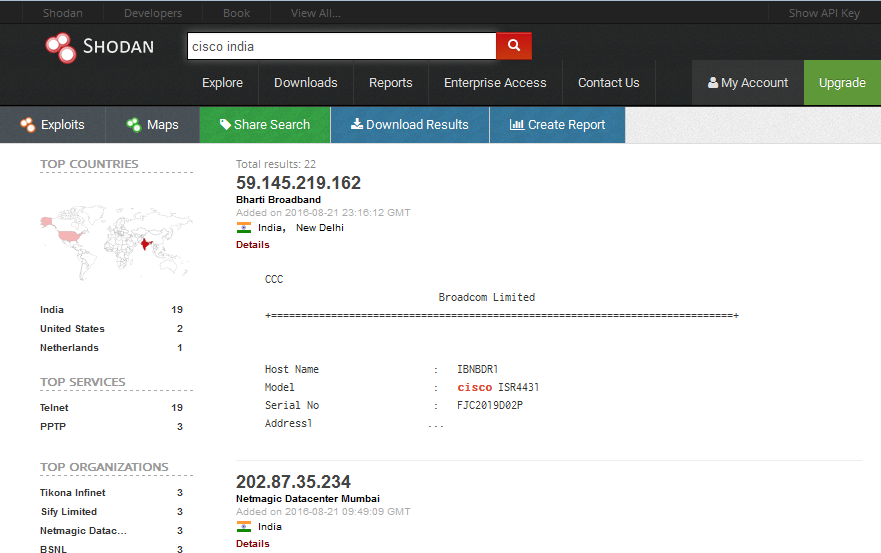
1. **Traffic Signals**

Searching about traffic signals or traffic signals camera then it will show you all the traffic surveillance camera present.



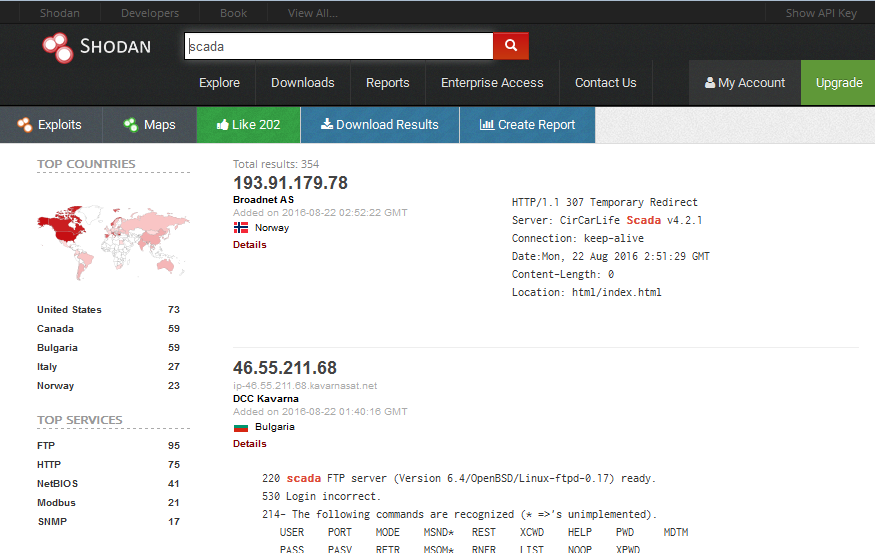
1. **Cisco**

Searching about cisco will show you all the cisco routers in the world but you can search them by country. Like, here, i have found cisco routers in India and result is below image :



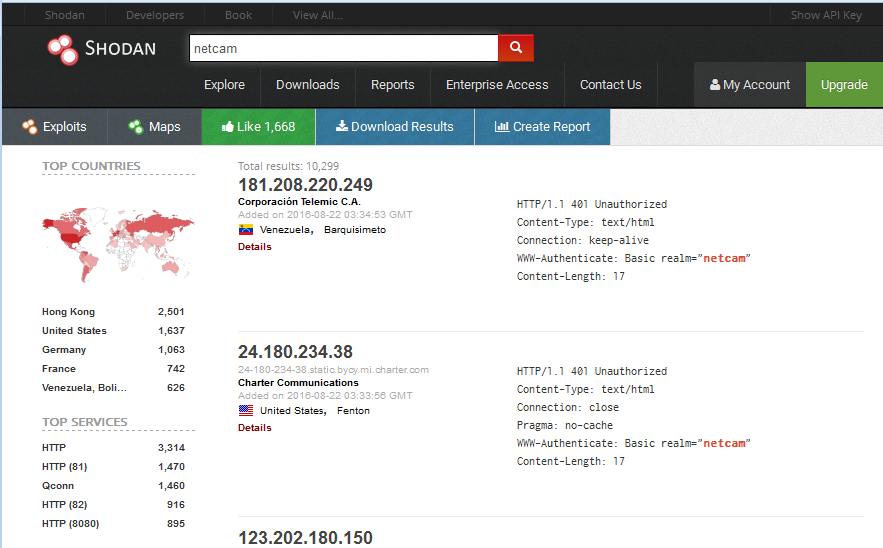
1. **Scada**

You can also search about Scada and you will get its information around the whole world as shown :



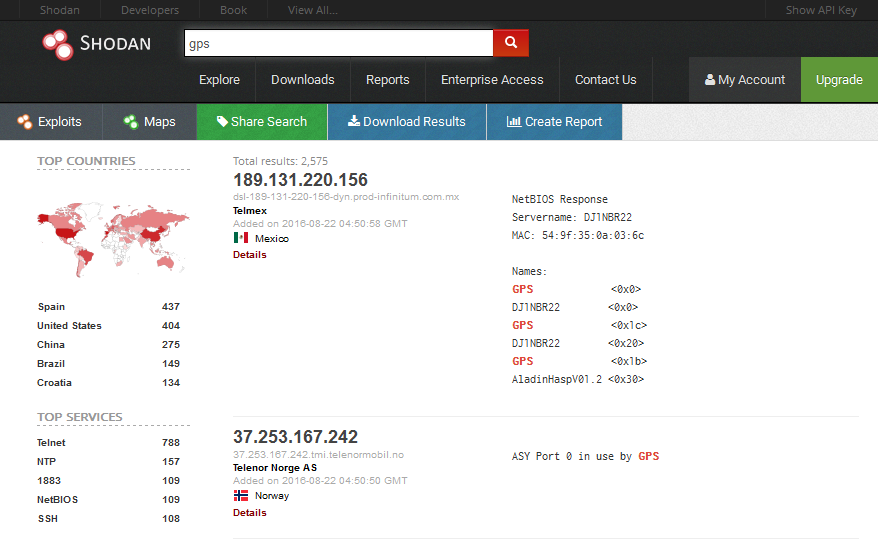
**netcam**

Shodan can also show you about all the netcams in world and you can access them too with your hacking skills.



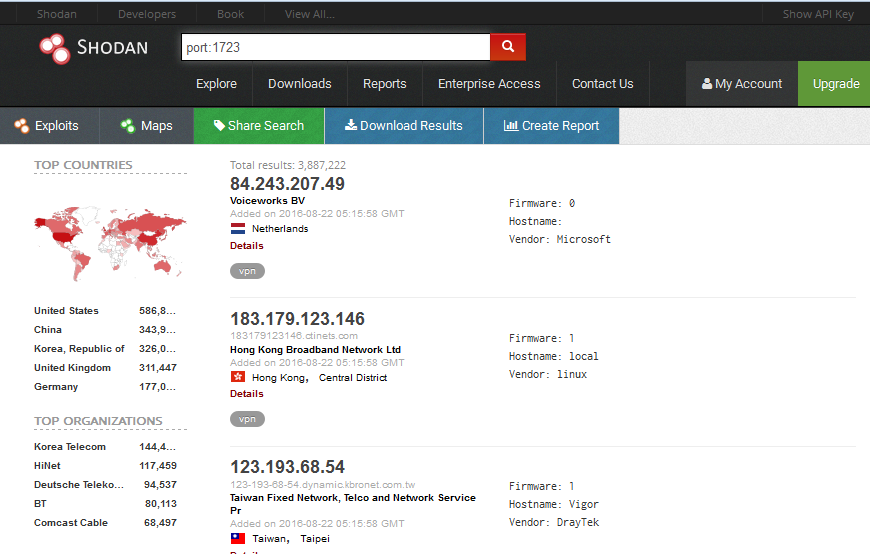
**GPS**

Shodan even lets you find all the GPS devices all over the world and for this you just have to type gps in the search box.

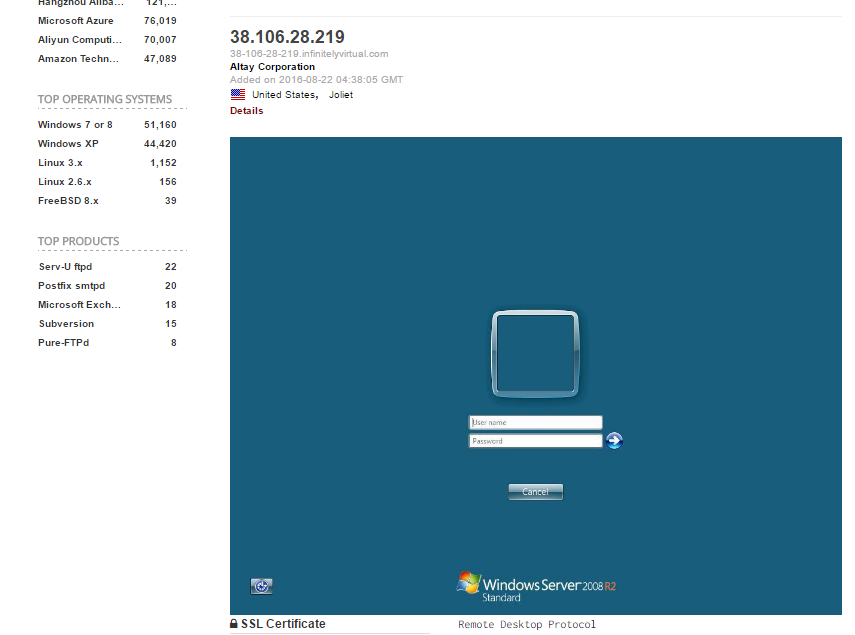


**Port**

Not only the devices but it can help find which port is open in which device. For example I have here searched port : 1723. Now we all know this port is used for VPN so through this we can know which device is using VPN as shown in image below :



When you search for port : 3389 it will show the operating system used by the device too which can be very useful.



This is how Shodan is useful for hackers as it gives all the information necessary to collect that too all over the world. And so you can manipulate this information as you desire.

**Integration with Metasploit Usage:**

i) Open Metasploit framework in Kali.

ii.)Type show auxiliary in the console

iii) Using the module auxiliary/gather/Shodansearch

iv) Now, we will see the parameters required by the auxiliary by using show options.