**Lab Experiment 04**

**B. Tech CSF-CSE Semester III Course: Physical and IT Security**

**By: Dr. Gopal Singh Rawat**

**Lab Objective: Find vulnerabilities in Live IoT devices on Internet**

**Tools:**

* Web Browser
* Shodan
* Netcraft

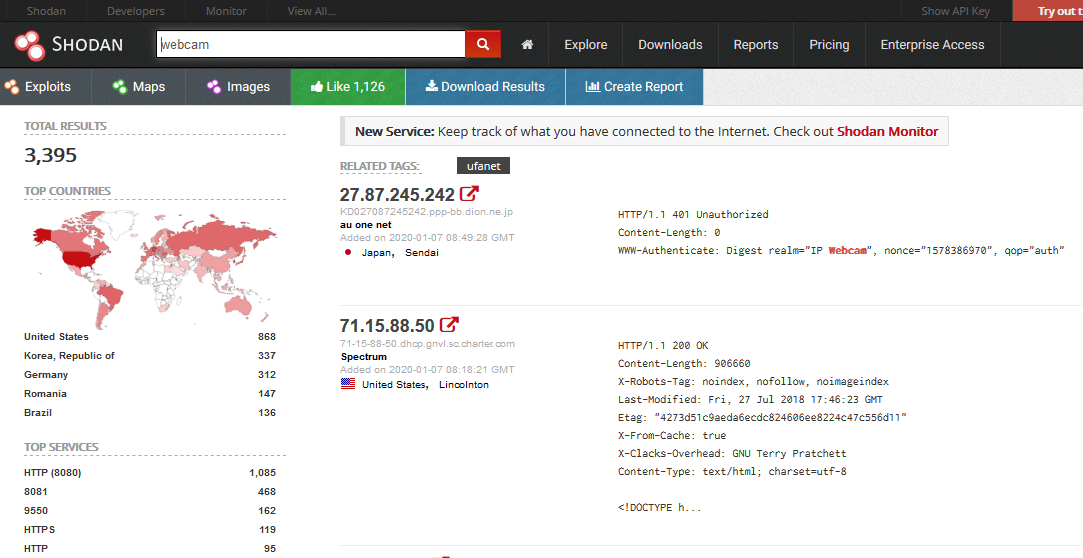
**IoT Devices or Internet of Things (IoT)** is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

[**Shodan**](https://null-byte.wonderhowto.com/collection/shodan-guides/) is an IoT search engine, indexes nearly every device connected to the Internet. Displays as easy-to-search database, giving hackers access to vulnerable devices online across the globe, you can search its database via its website or command-line library.

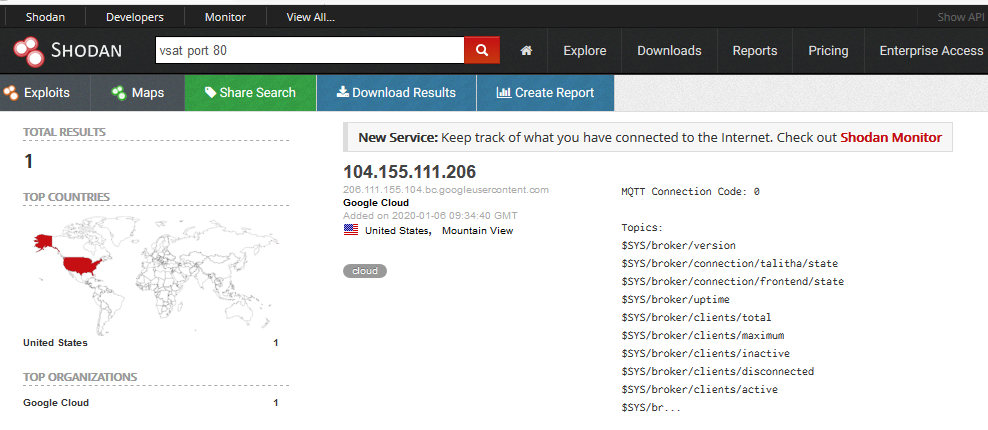
**Netcraft** provides details regarding Site/Domain reputation, Cybercrime Trends, Phishing (Countries, Hosters, Map, Bad Certificates for SSL), Popular Web sites, Takedown Map.

**Steps to perform:**

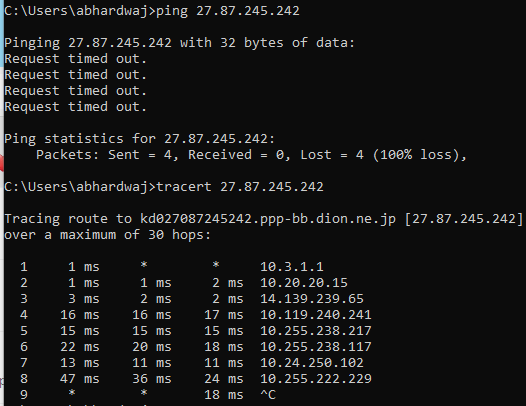
1. **Using SHODAN:** Open Web Browser 🡪 [www.shodan.io](http://www.shodan.io/) and Login to Shodan (free account)
2. Search keywords in Shodan browser for IoT sources 🡪 *washing machine, watch, music, IP webcam, webcam, printer, traffic controller, Netflix*



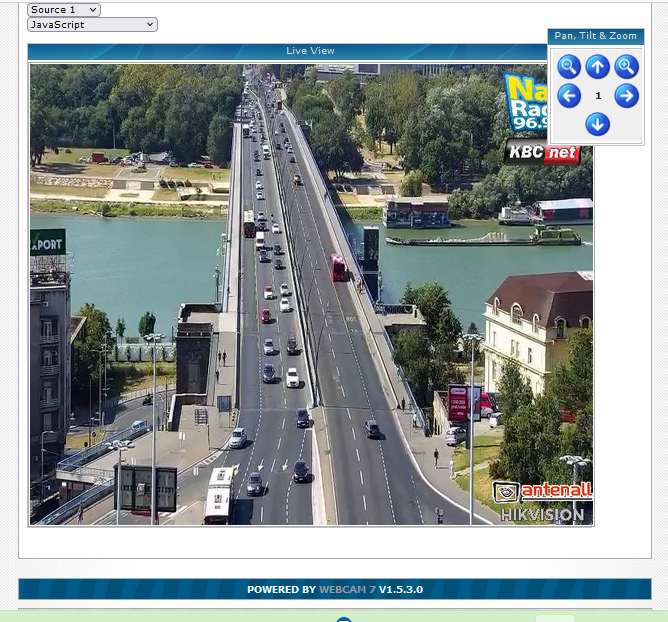
1. E.g. Search 🡪 VSAT port 80



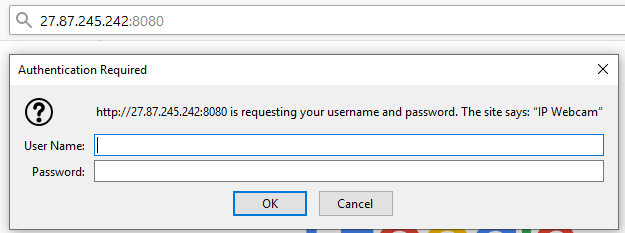
1. Open IP Addresses listed and check if the devices are LIVE 🡪 (Ping and Tracert) to detect the availability. Note 🡪 if PING/ICMP is blocked, you’ll get request timed out.



1. Copy the IP from the Shodan List and open it as per the ports mentioned in your web browser.
2. Example



1. Check if you can reach to the device admin page



1. Default username and passwords of some of the most widely used webcams below OR search for Setup Guide of that device on Google.

|  |
| --- |
| **ACTi**: *admin/123456* or *Admin/123456* |
| **Axis (traditional)**: *root/pass*, |
| **Axis (new)**: requires password creation during first login |
| **Cisco**: No default password, requires creation during first login |
| **Grandstream**: *admin/admin* |
| **IQinVision**: *root/system* |
| **Mobotix**: *admin/meinsm* |
| **Panasonic**: *admin/12345* |
| **Samsung Electronics**: *root/root* or *admin/4321* |
| **Samsung Techwin (old)**: *admin/1111111* |
| **Samsung Techwin (new)**: *admin/4321* |
| **Sony**: *admin/admin* |
| **TRENDnet**: *admin/admin* |
| **Toshiba**: *root/ikwd* |
| **Vivotek**: *root/<blank>* |
| **WebcamXP**: *admin/ <blank>* |

1. **Using Netcraft:** open <https://toolbar.netcraft.com/>
2. Search about any web site’s reputation 🡪[What's that site running? | Netcraft](https://sitereport.netcraft.com/)
3. Report a Phishing Web site or domain 🡪 <https://report.netcraft.com/report>
4. Find out Phishing Trends:
   1. Top Phishing Leaders 🡪 <https://report.netcraft.com/stats/leaderboard>
   2. Phishing Map 🡪 <https://trends.netcraft.com/cybercrime/map>
   3. Maximum Phishing Incidents 🡪 <https://trends.netcraft.com/cybercrime/countries>
   4. Most Popular Web Sites 🡪 <https://toolbar.netcraft.com/stats/topsites>

Examples

* <http://86.47.227.216:81/top.htm?Currenttime=2015-08-19%2005:28:15>
* [webcam 7](http://109.206.96.58:8080/home.html)

**Lab #04 File Work:**

1. Perform this Experiment and check to find at least 5 different Live vulnerable IoT devices
2. Capture the following for those devices as

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IP Address** | **Device** | **Open Ports** | **Geolocation** | **Mode/Make** | **Product Version** | **Admin Password** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Bonus: Report any device with admin page having default username and password.