# IoTVulnScan

Welcome To IoTVulnScan...

This software will scan with shodan API for all the IP addresses that are using vendors from RouterSploit.

Shodan site = https://www.shodan.io/

RouterSploit Github = https://github.com/threat9/routersploit

The software extracts the IP addresses with the countries and organizations for each IP and save it in IoTDevices.db file.

After it get all the IP addresses it needs, it starts to search for vulnerabilities for each IP with RouterSploiut.

If it found vulnerability in IP it will save the IP address in ScansReport.log file with the relevant RouterSploit vulnerability, the country and organization of the IP and the time it was found.

When the software ends it will delete routersploit.log and IoTDevices.db files.

Anyone looking for IoT devices with vulnerabilities should use this software.

You don't need any special skills to run it.

Just run it with the commend "bash IoTVulnScan.sh" or add execute option to the software and run it with "./IoTVulnScan.sh".

Before you can use the software you need to run the Install.sh script, it will install all the necessary stuff for IoTVulnScan software.

The Install.sh will install python 3 pip, shodan api, api key (You need to input the shodan API key before the run), RouterSploit requirements.

To input the shodan API key you just need to enter this commend to run the script:
bash Install.sh API_KEY
API_KEY = your API key in shodan.

When the Install.sh script is done it will print “Install Successful =]”.

You need to run the Install.sh script with root permissions.

# Screenshots ot the software

When the software scan for specific vendor IoT devices in shodan:

```
Scan for dlink IoT devices in shodan
[+] 100 IP addresses found
Shodan scan for dlink IoT device done
```

For example here I scanned for dlink IoT devices and the software find 100 IP addresses of IoT devices.

When the software finish to scan for IoT devices and scan each IP in RouterSploit to find vulnerability:

```
Start scan [redacted]
[-] Don't find vulnerability
Scan [redacted] done
Start scan [redacted]
[-] Don't find vulnerability
Scan [redacted] done
Start scan [redacted]
[-] Don't find vulnerability
Scan [redacted] done
Start scan [redacted]
[+] Find vulnerability
Scan [redacted] done
IoT vulnerability scan done.
```

For example I gave a file for the program with 4 IPs and there is a vulnerability in the last IP.

Screenshot of the ScansReport.log file with the vulnerability it found:

```
IP = [redacted]
Relevant RouterSploit vulnerability: http exploits/cameras/xiongmai/uc_httpd_path_traversal
Country: IL
Organization: Test
Time: 08/02/2021 18:51
```