**‘Exploring Shodan and Maltego’**

Ethical Hacking (S2-20\_SSZG575)

Assignment-1

|  |
| --- |
| Submission by: |
| **Pruthvirajsinh Rasikbhai Solanki (2020MT12018)** |

**Work Integrated Learning Program**



**BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI**

**February, 2021**

**Table of Contents**

[1. Context 3](#_Toc64386424)

[2. Assumptions 3](#_Toc64386425)

[3. Shodan 3](#_Toc64386426)

[3.1 Tool Overview and Capabilities 3](#_Toc64386427)

[3.2 Prominent Features 6](#_Toc64386428)

[3.2 Practical Examples 10](#_Toc64386429)

[**3.2.1** **Exploit Open Jenkins portal available in Ahmedabad, Gujarat, India.** 10](#_Toc64386430)

[**3.2.2** **Exploit Android Root Bridge** 11](#_Toc64386431)

[**3.2.3 Exploit Chromecast In India** 12](#_Toc64386432)

[4. Maltego 14](#_Toc64386433)

[4.1 Tool Overview 14](#_Toc64386434)

[4.2 Manual FootPrinting City Website 15](#_Toc64386435)

[4.3 Check Email Address Compromising 16](#_Toc64386436)

[4.4 Exploring Fingerprint L3 17](#_Toc64386437)

[5. References 19](#_Toc64386438)

# 

# 1. Context

As a part of Ethical hacking assignment, following is my exploration on SHODAN (Sentient Hyper Optimized Data Access Network) and Maltego. This report contains all necessary information along with assumptions and reference I took to complete the exercise.

# 2. Assumptions

* Intentionally I didn’t conduct further exploitation using tools like Ghost Framework or ChromeCast Exploitation Kit because of Security Reasons.
* I excluded couple of trivial Shodan searches assuming it is straight forward and easy to lookup. I opted to mentioned only key searches which can help in further exploitation if needed.
* Maltego CE edition provides very limited free transforms plus many of them requires API Keys. Because of this I was not able to dig deeper. Some scans are also restricted because of security issues or legal aspects.

# 3. Shodan

Shodan is a search engine for internet connected devices. It allows you to explore the internet, see a big picture, gain a competitive advantage, or monitor network security. The Shodan search engine is simple to use and should be familiar to most internet users. It functions in a manner similar to Google, DuckDuckGo, or other search engines. You can look for specific items or search for keywords.

## 3.1 Tool Overview and Capabilities

According to John Matherly, creator of Shodan, it is the scariest search engine on the Internet. Unlike Google, which crawls the Web looking for websites, Shodan navigates the Internet's back channels. It's a kind of "dark" Google, looking for the servers, webcams, printers, routers and all the other stuff that is connected to and makes up the Internet. Shodan runs 24/7 and collects information on about 500 million connected devices and services each month

It's stunning what can be found with a simple search on Shodan. Countless traffic lights, security cameras, home automation devices and heating systems are connected to the Internet and easy to spot.

Shodan searchers have found control systems for a water park, a gas station, a hotel wine cooler and a crematorium. Cybersecurity researchers have even located command and control systems for nuclear power plants and a particle-accelerating cyclotron by using Shodan.

**How Shodan Works**

Shodan is a close source project. However, Shodan themselves have declared that they use a ‘home-grown, distributed port scanner’ in order to search the internet. There exist approximately 4,294,967,296 (four billion two hundred ninety-four million nine hundred sixty-seven thousand two hundred ninety-six) IPv4 Addresses. This pool is 32-bits in size. Scanning these addresses is an embarrassingly parallel workload and can be easily distributed over any number of systems. The term embarrassingly parallel simply means that little or no effort is needed to separate this problem into a number of parallel tasks.

**The Banner**

Devices run services and those services are what Shodan collects information about. For example, websites are hosted on devices that run a web service and Shodan would gather information by speaking with that web service. The information for each service is stored in an object called the banner. It is the fundamental unit of data that Shodan gathers and what you'll be searching for. A simplified banner looks like the following:

|  |  |
| --- | --- |
| **Banner** | **Explanation** |
| {  "data": "Moxa Nport Device  Status: Authentication disabled  Name: NP5232I\_4728  MAC: 00:90:e8:47:10:2d",  "ip\_str": "46.252.132.235",  "port": 4800,  "org": "Starhub Mobile",  "location": {  "country\_code": "SG"  }  } | The given banner has 5 properties but a real banner will contain many more properties and detailed information about the service. Each property stores a different type of information about the service:   * data: the main response from the service itself * ip\_str: IP address of the device * port: port number of the service * org: the organization that owns this IP space * location.country\_code: the country where the device is located |

**By default, the Shodan searches “data” property only**, so to search about other properties of the banner, user must use set of filters values as query parameters. The syntax should be like “filtername:value”. For example,

|  |  |
| --- | --- |
| **Filters** | **Output** |
| Country: IN  *i.e., Devices located in India* |  |
| org:BSNL city:Vadodara  *i.e., BSNL devices running in City Vadodara, Gujarat.* |  |
| product:"Counter-Strike Global Offensive" country:IN  *i.e., PC game “Counter Strike Global Offensive” servers running across india* |  |

## 3.2 Prominent Features

Following can be considered as “Prominent features” of Shodan.

1. **Service Banner with vast Meta data and Ports scanning abilities**

Service banners contain all the metadata related to a specific device. Following are some of the key information that the service banner metadata can provide.

|  |  |
| --- | --- |
| **Information** | **Ports** |
| * Geographic location * Default username and passwords * IP address * Software version * Make and model | * Port 554 – Real Time Streaming Protocol * Port 5060 – SIP * Port 25 – SMTP & Port 161 – SNMP * Port 23 – Telnet * Port 993 – IMAP * Port 22 – SSH * Port 21 – FTP * Ports 8443, 443, 8080, and 80 – HTTPS/HTTP |

1. **Vulnerability detection and Security Awareness**

Shodan can be considered as a primary resource for vulnerability assessment and penetration testing because one can take advantage of the various filters that Shodan offers. Using filters like Geography (country, city, coordinates), Hostname, Network (IP or /x CIDR), Port, Operating System, Time Frame etc. With these, you can easily search your network for open ports, default credentials, and unnecessary online connections that are making your network vulnerable to attacks.

Apart from this, when security researchers uncover new, sophisticated exploits, Shodan can search for those known vulnerabilities across your connected devices to ensure that any steps you’ve taken for remediation were 100% effective.

1. **Shodan API**

Apart from the Web user interface, Shodan also provides APIs to request and receive data from the search engine directly, automating some of the security operations that we need to perform. As the IoT continues to scale exponentially, this may help in automating as many VA/PT operations as possible to keep pace with growing security demands.

1. **Community Generated Searches**

For beginners, Shodan provides shared search directory. Here, users can mark and share certain search queries they find interesting or useful. People are able to readily describe, tag and share their search queries for others to use.

1. **Result Mapping**

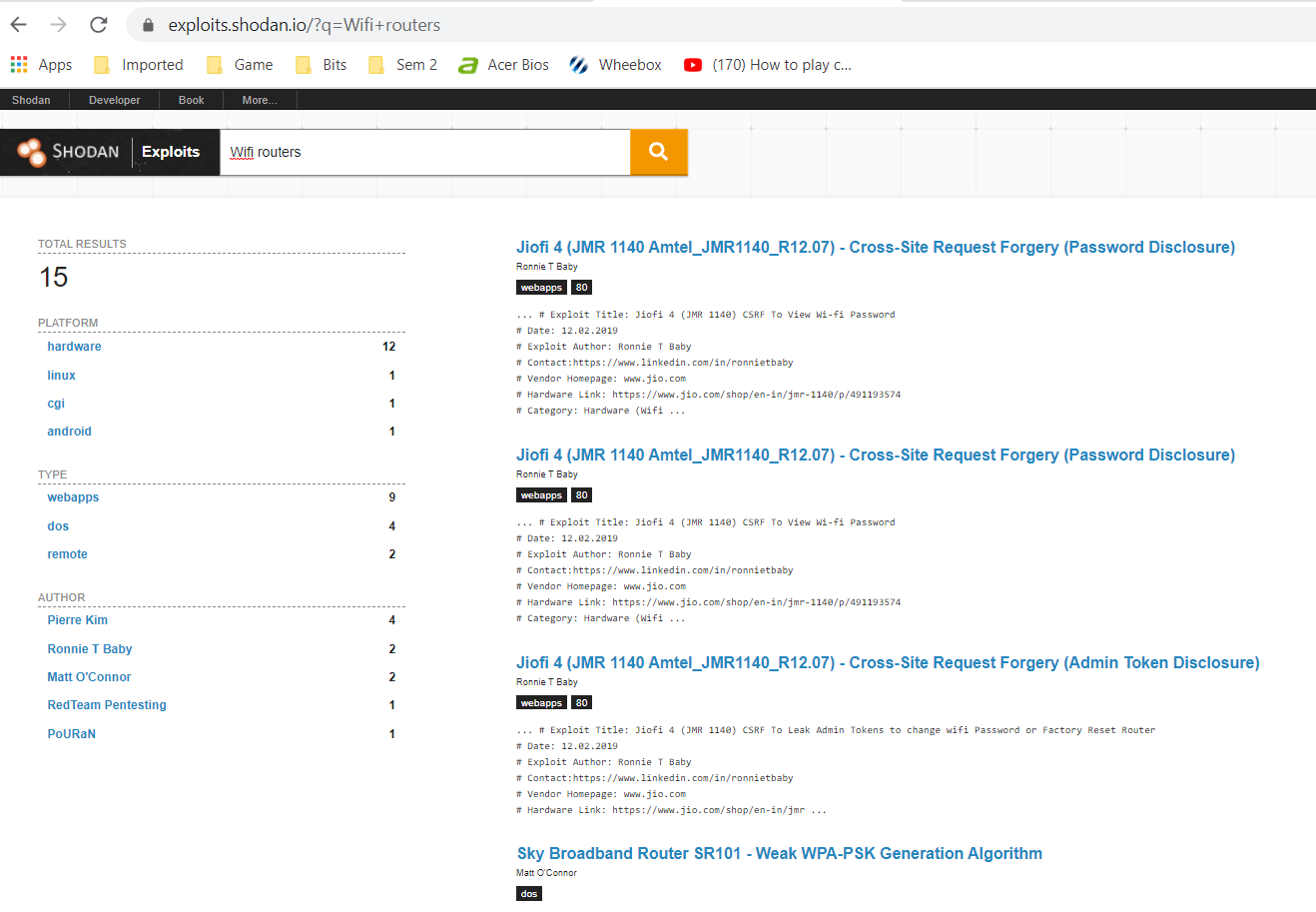
In some cases, a visual is easier to read and gives more information than plain text. See hundreds of results in one screen and differentiate each by location at a glance with Shodan’s Maps feature. As per <https://shodanio.wordpress.com/2014/02/18/introducing-shodan-maps/>

, following are some of the Map views Shodan can provide. However, it is paid service. User can filter the searches based on panning of the maps, narrowing it down to particular region or area.

|  |  |
| --- | --- |
| Globally exposed Routes having Backdoor |  |
| Street view of the same |  |

1. **Exploit Tracking**

Shodan collects various digital exploits and vulnerabilities from sources like Exploit DB, CVE, and Metasploit and provides them through a web search interface. See <https://exploits.shodan.io/welcome>. For example, following shows list of exploits noted down for Wi-Fi routers.



1. **Status Report**

For any search query, you can take a snapshot of how the search results are distributed online at that time. The free reports Shodan generates provide a general overview of the results shown through detailed graphs and charts.

1. **Integrations**

Shodan does provide integration with other tools like:

* Web browser plugins compatible with Chrome and Firefox.
* Maltego, an open-source application for exploring large amounts of data.
* Command-line interface, packaged with Shodan’s own set of commands.

## 3.2 Practical Examples

I have explored couple of filters and look under community generated searches to prepare couple of commands to explore Shodan. I have divided my searches into following scenarios to group them better.

### **3.2.1** **Exploit Open Jenkins portal available in Ahmedabad, Gujarat, India.**

* **Search Query:** <https://www.shodan.io/search?query=%22X-Jenkins%22+%22Set-Cookie%3A+JSESSIONID%22+http.title%3A%22Dashboard%22+country%3AIN+city%3A%22Ahmedabad%22+product%3A%22Jetty%22>
* **Search filters:**  *"X-Jenkins" "Set-Cookie: JSESSIONID" http.title:"Dashboard" country:IN city:"Ahmedabad" product:"Jetty"*
* **Search Output**

|  |  |
| --- | --- |
| Shodan output |  |
| Open URL | <http://27.109.9.122:8080/>  I am able to locate Jenkins job running on this website and can manipulate the code but I stooped at this point because of security reasons. |
| whois 27.109.9.122 |  |

### **3.2.2** **Exploit Android Root Bridge**

Android Debug Bridge (ADB for short) which allows developers to communicate with a device remotely, to execute commands and fully control the device. However, It is completely unauthenticated, meaning anybody can connect to a device running ADB to execute commands. Unfortunately, vendors have been shipping products with Android Debug Bridge enabled. It listens on port 5555, and enables anybody to connect over the internet to a device. I have explored couple of devices open in India.

Furthermore, using Ghost framework in Kali Linux, we can connect to any such devices and perform operations like screen capture, install and uninstall application etc.

In my case, I need to stop at this point because all devices shown by Shodan were almost gone offline at night.

* **Search Query:** <https://www.shodan.io/search?query=%22Android+Debug+Bridge%22+%22Device%22+port%3A5555+country%3AIN>
* **Search filters:**  *"Android Debug Bridge" "Device" port:5555 country:IN*
* **Search Output**

|  |  |
| --- | --- |
| Shodan output |  |
| Ghost Framework |  |

### **3.2.3 Exploit Chromecast In India**

I was able to find 3 Chromecast connected in India. Following are my results. It can be further exploited using ChromeCast Exploitatin Kit but I didn’t try that considering security concerns.

* **Search Query:** <https://www.shodan.io/search?query=%22Chromecast%3A%22+port%3A8008+country%3AIN>
* **Search filters:**  *"Chromecast:" port:8008 country:IN*
* **Search Output**

|  |  |
| --- | --- |
| Shodan output |  |

# 4. Maltego

## 4.1 Tool Overview

Maltego is software used for open-source intelligence and forensics, developed by Paterva from Pretoria, South Africa. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.

Maltego permits creating custom entities, allowing it to represent any type of information in addition to the basic entity types which are part of the software. The basic focus of the application is analyzing real-world relationships (Social Networks, OSINT APIs, Self-hosted Private Data and Computer Networks Nodes) between people, groups, Webpages, domains, networks, internet infrastructure, and social media affiliations. Maltego extends its data reach with integrations from various data partners.[4] Among its data sources are DNS records, whois records, search engines, social networking services, various APIs and various meta data.

Following are some of the key terminology of Maltego worth to note.

|  |  |
| --- | --- |
| **Terminology** | **Meaning** |
| Entity | * An Entity is a piece of information shown as a node on the graph. Entities may have multiple types * For example, DNS name, Person name, Phone number, etc. The Maltego Client comes with about 20 Entities targeted for use in online investigations. |
| Transform | * piece of code that searches for information related to an Entity on the graph * Transforms allow you to query an API or database to show related info on the graph. * For example, we could have the website "www.maltego.com" and transform it into the IP address "104.248.60.43" |
| Machine | * Machines are the Maltego equivalent of macros. Machines allow you to chain together multiple Transforms, filters and actions in order to automate common and tedious tasks |
| Hub Item | * Transforms and the Entity types that the query need to be stored on a server that can be accessed by the Maltego Client. |

## 4.2 Manual FootPrinting City Website

Just for the assignment sake, I am using my city website [www.bardoda.com](http://www.bardoda.com) to see what details I can find out using Maltego about it. See step by step process below.

|  |  |
| --- | --- |
| * Add Domain “baroda.com” * Map it to the website |  |
| * Found ip Address * Then I ran Shodan – Basic details transformation to get the idea about what is there on given ip. * Where I found couple of ports, DNS server and other info. |  |
| * Using the ip Address, I found NetBlock. * From the Netblock, I scan for AS Number there I went for Companies that are connected.   I stopped my exploration to this point because of security reasons. |  |

## 4.3 Check Email Address Compromising

Using “Have I been Pwned” transformation tool, I have tried to scan through my personal email address to check whether it is compromised or not.

To achieve this efficiently, instead of applying multiple transformation manually, I used “@haveibeenpwnd ..” machine.

|  |  |
| --- | --- |
| * Configure the machine |  |
| * Outcome of the initial lookup * My email address is being used by Gaadi.com, Dubmash.com etc. website. Soon I will be blocking those access. |  |

## 4.4 Exploring Fingerprint L3

I wanted to explore the built-in Machine that can done Fingerprinting L3, i.e. (intense and the most complete information gathering on any target.

See my finding below.

|  |  |
| --- | --- |
| * Configure Machine and run |  |
| * It provided lots of information |  |
| * On the ip available, I ran Shodan transform |  |
| * I tried to run Shodan Vulnerability scan on multiple entities but most of them are returning 0 data.   So, I stopped at this point. |  |

# 5. References

For Shodan:

* [Introduction to Shodan by Aron Jones](https://www.youtube.com/watch?v=01dLzan9g0E&list=PLLC0M-nds_-SkVxNcMleRfrfNTfv9V1zF&index=9)
* <https://www.shodan.io/home>
* <https://en.wikipedia.org/wiki/Shodan_(website)>
* <https://money.cnn.com/2013/04/08/technology/security/shodan/>
* <https://www.safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/>
* <https://doublepulsar.com/root-bridge-how-thousands-of-internet-connected-android-devices-now-have-no-security-and-are-b46a68cb0f20>
* <https://medium.com/cyber-security-resources/remotely-access-android-device-by-exploiting-adb-using-ghost-framework-8356afe09c2e>
* <https://www.brussec.com/2019/01/11/hacking-chromecasts-for-fun/>

For Maltego:

* <https://en.wikipedia.org/wiki/Maltego>
* <https://docs.maltego.com/support/solutions/articles/15000008829-glossary-of-terms>
* [Maltego - Automated Information Gathering](https://www.youtube.com/watch?v=zemNLx0-LRw)
* <https://null-byte.wonderhowto.com/how-to/hack-like-pro-use-maltego-do-network-reconnaissance-0158464/>