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. On the next screen, click the **Register** button on the menu bar. Fill in your information to create a Shodan account. You will receive an email to activate your account.
d. 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.

According to Shodan, what is the fundamental unit of data it gathers?

Answer Area

```
<!----><!---->
```

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?

Answer Area

```
<!----><!---->
```

c. 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?

Answer Area

```
<!----><!---->
```

d. 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?

Answer Area

```
<!----><!---->
```

What information is available for the open ports?

Answer Area

```
<!----><!---->
```

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. Try searching on some manufacturer names in Shodan. From the results, you can refine your search results, sometimes with specific manufacturer’s model numbers. In addition, search for default logins used by camera model. It is possible that the owner of camera did not change the default password. **DO NOT** attempt to login to devices that you do now 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
```

a. 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
```

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
```

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.

How many FTP servers did Shodan find in San Jose that permitted anonymous logins?

Answer Area

<!----><!---->

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

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

What additional information is contained in the General Information section when compared to the result you recorded in Step 1c?

Answer Area

<!----><!---->

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.

a. 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.

b. Shodan is a Python library that is installed in Kali by default. Open a Kali terminal window.

c. 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.

```
┌──(root㉿kali)-[/home/kali]

└─$ shodan init <paste your API key here>
```

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.

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.

```
┌──(kali㉿kali)-[~]

└─$ shodan search webcam
```

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.

Step 2: Execute other Shodan CLI commands.

a. 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.

```
┌──(kali㉿kali)-[~]

└─$ shodan info

Query credits available: 0

Scan credits available: 0
```

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

b. 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.

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
```

   This query returns the summary statistics for the webcam search.

Reflection Question

Shodan can provide a wealth of information about systems and devices that are connected and communicating on the internet. What features of Shodan are especially valuable for IT administrators?

Answer Area

```
<!----><!---->
```