OSINT-SPY

Release 2.0.0

Jan 31, 2020

OSINT-SPY Command Line

CHAPTER 1

Overview

Starting from Espionage and ending at OSINT, our data gathering techniques has been developed magnificently. In 90's, the security posture of national security, law enforcement agencies, Cyber Security agencies was totally different. At that time, gathering data about someone was very difficult due to fewer Internet resources. But, this digital era has overcome the techniques used for information gathering in 90's by Intelligence Gathering. It includes gathering data from various public sources and their API. Intelligence Gathering includes human, geo-location, open-source, signals, digital and financial intelligence.

OSINT-SPY can find information about a person, email, an organization, person's geolocation, domain names, publically available devices on the internet and so on. It can be used by Data Miners, Infosec Researchers, Penetration Testers and Cyber Crime Investigators in order to find deep information about their target.

CHAPTER 2

Setup

Installing and using OSINT-SPY is very easy. Installation process is very simple and is of 4 steps.

1. Downloading or cloning OSINT-SPY github repository.
2. Downloading and installing all dependencies.
3. Generating API Keys
4. Adding API Keys in config file

Let's Begin !!

2.1 Cloning Osint-Spy

In order to install OSINT-SPY simply clone the github repository. Below is the command which you can use in order to clone OSINT-SPY repository.:

```
git clone https://github.com/SharadKumar97/OSINT-SPY.git
```

2.2 Installing dependencies

Once you clone OSINT-SPY, you will find one directory name as OSINT-SPY. Just go that directory and install the requirements either in a virtual environment or in the system itself.

```
pip install -r requirements.txt
```

CHAPTER 3

Generating API Keys

We need some API Keys before using this tool. Following are the API's which we are using in this tool for a time being. Paste all the API keys in the config.py in their respective placeholdes.

3.1 Clearbit API

1. Create an account at Clearbit. Fill in the email address and password.
2. Click Next. Fill in the relevant details.
3. Confirm your email address.
4. You will notice **API Key** in **API section** in left pane. Copy that and paste in `clearbit_api_key`.

3.2 Shodan API

1. Create an account at Shadon. Fill in the details.
2. Confirm the email address.
3. Login with the credentials.
4. After login, you will notice **API Key** in **Account Overview** section. Copy that and paste in `shodan_api_key`.
5. If successfully logged in, the **API Key** is also visible at the topmost header of shadon.io.

3.3 FullContact API

1. Create an account at FullContact. Use your business email address.
2. Fill in the required details.

3. After successfully logging in, select Get an **API Key** from **Getting started** section.
4. Enter the name for the key and after generating, paste the key in `fullcontact_api_key`.

3.4 VirusTotal API

1. Create an account at VirusTotal. Fill in the details.
2. Confirm your email address. Log in to your account.
3. Click on the avatar on top right to visit your profile.
4. You will notice an **API Key**. Paste that key in `virus_total_api_key`.

3.5 Email Hunter API

1. Create an account at Email Hunter. Use your business email address.
2. Fill in the details. Confirm your email address. Verify your mobile number.
3. After successfully logging in, find your **API Key** under your profile in top right.
4. Paste that API key in `email_hunter_api_key`.

CHAPTER 4

Usage

OSINT-SPY is very handy tool and easy to use. All you have to do is just pass values to parameter. Use `--json` to generate output in json format. In order to start OSINT-SPY just write

```
python osint-spy.py
```

4.1 –btc_block

–btc_block parameter gives you the information of the latest bitcoin block chain. Optional Parameter `--json`

```
python osint-spy.py --btc_block
```

or

```
python osint-spy.py --btc_block --json
```

4.2 –btc_date

–btc_date parameter will give you an information of bitcoin block chain from given date. Optional Parameter `--json`

```
python osint-spy.py --btc_date 20170620
```

or

```
python osint-spy.py --btc_date 20170620 --json
```

4.3 –btc_address

–btc_address will give you an information about particular bitcoin owner. Optional Parameter `--json`

```
python osint-spy.py --btc_address 1DST3gm6JthxhuoNKFqXrdpzPFfz1WgHpW
```

or

```
python osint-spy.py --btc_address 1DST3gm6JthxhuoNKFqXrdpzPFfz1WgHpW --json
```

4.4 –ssl_cipher

-ssl_cipher will show you all the ciphers supported by given website.

```
python osint-spy.py --ssl_cipher google.com
```

4.5 –ssl_bleed

–ssl_bleed will find out whether given website is vulnerable to heartbleed or not ?

```
python osint-spy.py --ssl_bleed google.com
```

4.6 –domain

–domain will give you in depth-information about particular domain including whois, dns, ciphers, location and so more. Optional Parameter `--json`

```
python osint-spy.py --domain google.com
```

or

```
python osint-spy.py --domain google.com --json
```

4.7 –email

–email will gather information about given email address from various public sources. Optional Parameter `--json`

```
python osint-spy.py --email david@google.com
```

or

```
python osint-spy.py --email david@google.com --json
```

4.8 –device

–device will search for a given device from shodan and will list out all the available devices on public IP. Optional Parameter `--json`

```
python osint-spy.py --device webcam
```

or

```
python osint-spy.py --device webcam --json
```

4.9 –ip

–ip will gather all the information of given IP Address from public sources. Optional Parameter `--json`

```
python osint-spy.py --ip 127.0.0.1
```

or

```
python osint-spy.py --ip 127.0.0.1 --json
```

4.10 –malware

–malware will send a given piece of file to virustotal and will give you a result whether given file is malware or not? Optional Parameter `--json`

```
python osint-spy.py --malware abc.exe
```

or

```
python osint-spy.py --malware abc.exe --json
```

CHAPTER 5

Roadmap

This is the initial version of OSINT-SPY. In future, we will add various social platofrms API and we will try to make it better by adding database functionality.

Github Repository Link: OSINT-SPY.