Hashes Queries Script

Name: Abderrahim Mayaba
Position: SOC Analyst
Email: ammayaba@gmail.com

Introduction

Overview

Hashing is a cryptographic process that can be used to validate the authenticity and integrity of various types of input. It is widely used in authentication systems to avoid storing plaintext passwords in databases, but is also used to validate files, documents and other types of data. Incorrect use of hashing functions can lead to serious data breaches, but not using hashing to secure sensitive data in the first place is even worse.

Motivation

One of the information security practitioner duties is to inspect hashes (usually published on well-known resources or received by special resources such as NCA) and then block them. Some popular systems (like VirusTotal) are usually used for this purpose. However, querying large, or even small numbers every day, can be very exhausting and time consuming unless it is automated. Fortunately, VirusTotal has API that can be leveraged for this use. The main job of the script is to query the VirusTotal API with a list of given hashes.

Script Description

Specifications

The script has the following specifications:

- Read an input file that contains hashes from user.

- Query the provided hashes to VirusTotal.

- Display (in command line) the progress of the search.

- Get many information associated with the queried hash (for example: number of positives, type of the file, search engines detected the hash, and many other useful insights)

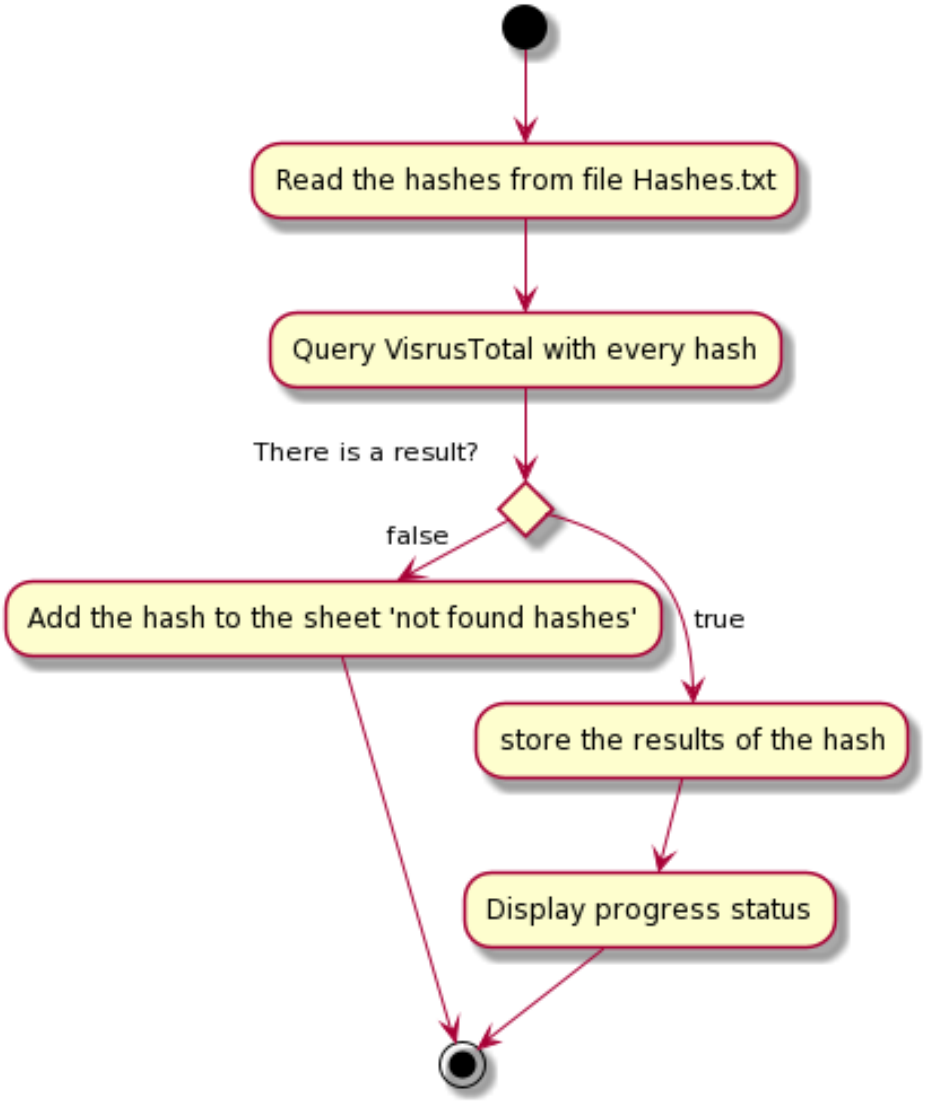
- Store the results in a structured excel file.

How to use the script

Make sure that you have python installed on your system before running the script, after that:

1- Enters the hashes in a txt file named “hashes.txt” at the same folder of the script (make sure the hashes are separated by new line).
2- Open the command line and run the file (by typing: python CheckHashes.py).
3- The script will display the progress of the search in the command line
4- An excel file with the name “HashResults” will be created on the same folder as the script that contains all the results

Execution logic flow



Future Work

There are many opportunities of improvements in the script (for example: adding a memory or other features like reading from emails). Also, there is a plan to extend the functionality of the script to give the user the option to query VirusTotal with IPs or URLs. In my point of view, there are many routine tasks that can be automated to make the duties of the SOC team easier and more efficient.