Assignment 13: VirusTotal API Usage

Report

Aim: Use VirusTotal's database to check if a file is malicious by analyzing its digital fingerprint.

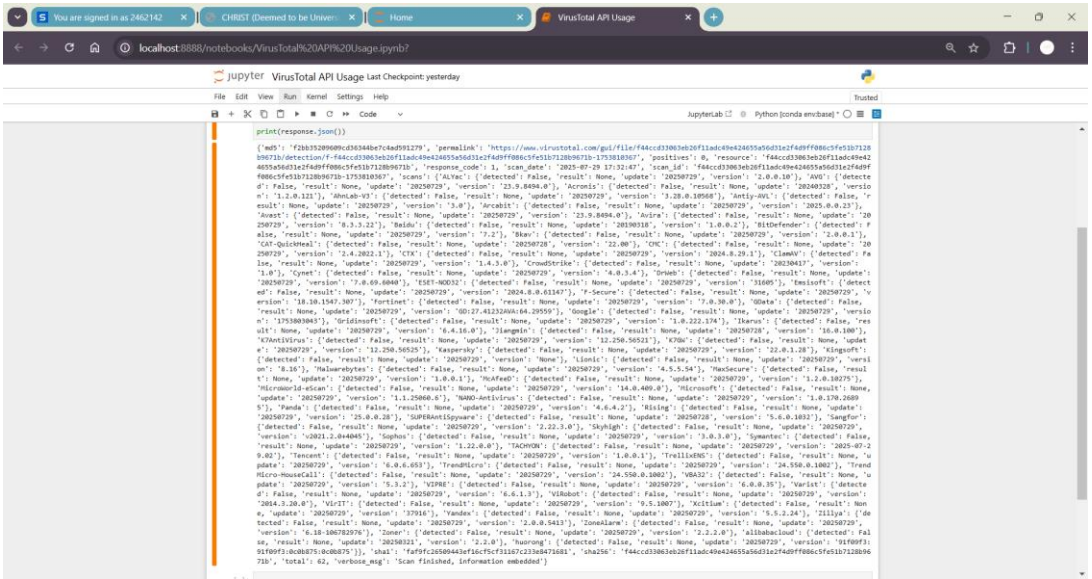
Methodology:

1. Create an API Key
    - Register for VirusTotal API key.
    - Go to the Profile in the VirusTotal website and access the API Key.
    - Copy the API Key.
2. Python code to check the file hash

```
import hashlib
import requests

file_path = "D:/L&T FrontEnd UI UX/CSS Notes.txt"
with open(file_path, "rb") as f:
    file_hash = hashlib.sha256(f.read()).hexdigest()

api_key = "3b6e82c7650df8ee7de9c4723c26ce1670f715b1c8298c7d4a16c75cbff188b2"
response = requests.post(
    "https://www.virustotal.com/vtapi/v2/file/report",
    data={"apikey": api_key, "resource": file_hash}
)

print(response.json())
```

3. Upload the file to be scanned on the VirusTotal Website
    - Click on the *Choose File* option.
    - Choose the file you want to scan.
4. Run the Python Program
    - Make sure to provide the correct file path of the file that has been scanned in VirusTotal.
    - If it's present in the same directory as the python file, we could include the relative path, or else provide the absolute path.
    - For the API Key, copy and paste the API Key obtained from the Profile in VirusTotal website.

Output



Findings:

Analysis

- **API Key Usage**: The code uses a (redacted) API key as required.
- **File Hashing**: Uses Python's hashlib to compute the SHA-256 hash, which is standard for VirusTotal.
- **API Call**: Uses requests.post to call the VirusTotal v2 API, sending the hash and the API key.
- **Prints Results**: The output JSON includes detection results from many antivirus engines.

The file's hash is checked and VirusTotal's multi-engine scan returns "detected: False" across all engines, suggesting the file is likely safe.

Conclusion

How Hash-Based Detection with VirusTotal Works

- **Hashing**: Any file can be uniquely identified by its hash (commonly SHA-256). This is a digital fingerprint.
- **Database Lookup**: VirusTotal's API allows you to query if a hash (file) is already known, and shows the verdict from >70 antivirus scanners.

This is a high-confidence and effective method for a security analyst to check a file's safety using VirusTotal's API.