Malware Detection Tool

Minor Project Submission

1. Introduction

This project focuses on developing a basic **Malware Detection Tool** that scans directories for suspicious files. The tool is designed to:

- Detect malware by **comparing file hashes** using SHA-256.
- Identify **executable files** with suspicious behaviors.
- Integrate **VirusTotal API** (if accessible) for further analysis.

2. Methodology

To implement the tool, the following steps were taken:

1. **File Hash Comparison:**
    - Compute SHA-256 hashes of files in a given directory.
    - Compare hashes against a list of known malware signatures.
2. **Detection of Suspicious Executables:**
    - Identify .exe and .dll files.
    - Scan for patterns associated with malware (e.g., unusual permissions, obfuscation).
3. **VirusTotal API Check (If Available):**
    - Submit file hashes for verification against VirusTotal's database.
    - Retrieve scan results if API access is granted.

3. Outcome

The tool was successfully developed and tested. The key results include:

- Correct **SHA-256 hash generation** and comparison.
- Identification of executable files and basic heuristic checks.
- VirusTotal API integration was limited due to API constraints but worked for allowed requests.

4. Conclusion

The **Malware Detection Tool** serves as a basic yet effective way to scan for potentially harmful files.

- The hash-based method was **accurate and fast** for detecting known malware.
- The heuristic analysis **flagged suspicious executables** but requires further refinement.

- **VirusTotal API integration** enhances detection, though API limits must be considered.