Malware Detection Tool

Introduction

Malware detection is crucial for maintaining system security. This project aims to develop a Python-based malware detection tool that scans directories to detect malicious files using hash signatures.

How It Works

The tool compares the SHA-256 hashes of files in a specified directory against known malware hashes stored in a database file. If a match is found, the file is flagged as potentially malicious.

Enhanced Code Explanation

1. **Importing Required Modules**: The tool uses `hashlib` for computing SHA-256 hashes and `os` for directory traversal. Additionally, `tqdm` is used for showing progress bars during scanning.
2. **Loading Malware Hashes**: Hashes are loaded from a file using the `load_malware_hashes()` function. It also handles errors such as missing files and empty lines efficiently.
3. **Computing SHA-256 Hash**: The `get_sha256()` function reads files in chunks to efficiently calculate the hash, minimizing memory usage. It also includes better error handling for permission issues.
4. **Scanning Directory**: The `scan_directory()` function recursively scans all files in the specified directory, computing their SHA-256 hashes and checking them against the malware database. A progress bar shows the scanning status in real-time.
5. **Alert Mechanism**: If a hash matches any entry in the malware database, the tool alerts the user, indicating potential malware.
6. **Enhanced Features**:
   - **Progress Indicator**: Implemented using `tqdm` for real-time feedback on scanning progress.
   - **Error Handling**: Enhanced to manage file read errors and permission issues gracefully.

How to Run the Tool

- Install `tqdm` using: `pip install tqdm`
- Prepare a file named `malware_hashes.txt` containing known malware hashes, one per line.
- Update the directory path in the `scan_directory()` function.
- Run the script using: `python malware_scanner.py`

Conclusion

This tool provides a basic yet effective approach to malware detection using hash signatures. With planned improvements, it can become a more powerful security solution.