Defensive Malware Scanner Tool- Lab Report

1. Introduction

In this lab task, I created a simple defensive tool that scans files and identifies suspicious items.
This activity helped me understand how basic detection works in cybersecurity and how file scanning is done.

2. Objective

The main objective of this task was to design a basic tool that can scan files, detect unusual elements, and show the result to the user in a simple way.

3. Tools Used

- Python
- Windows Operating System
- Notepad/VS Code / Command Prompt
- Basic file handling functions

4. Procedure

1.First, I created a Python file for the scanning tool.

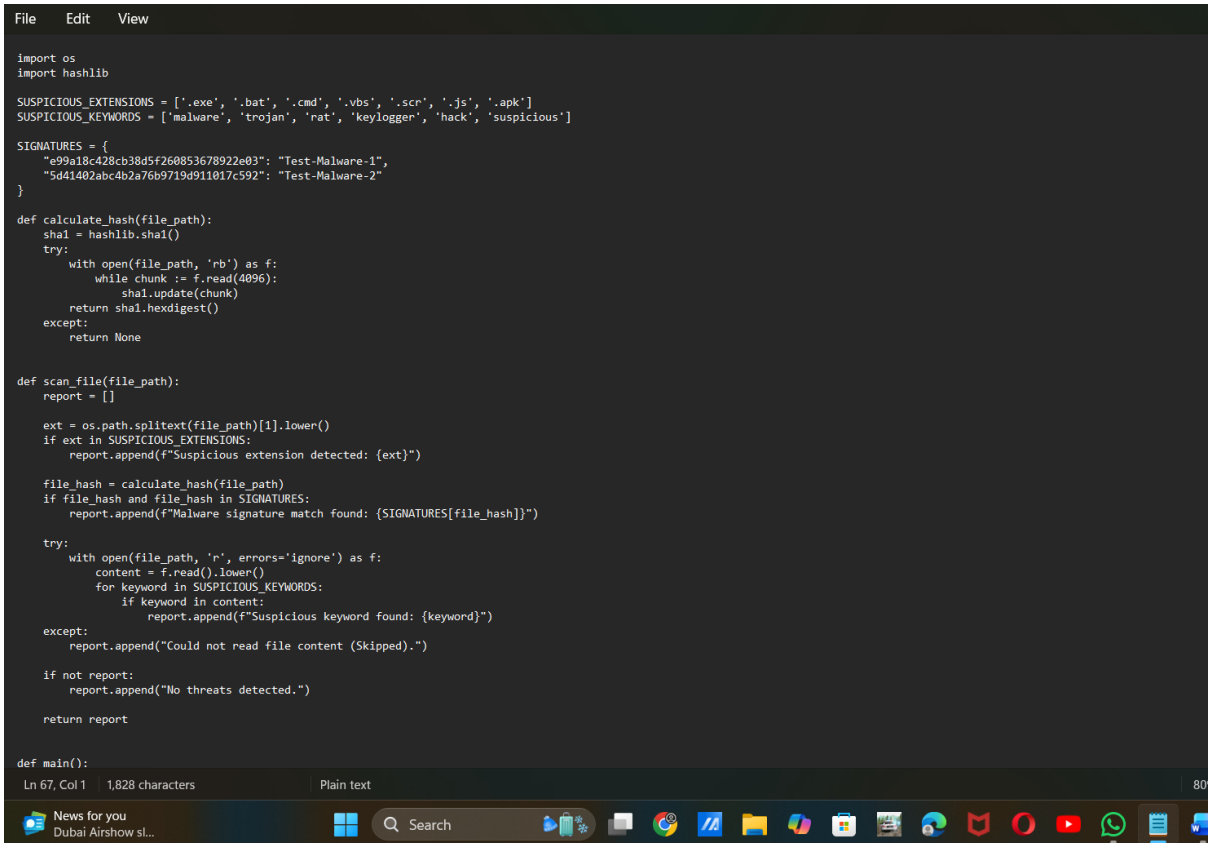
2. I added the code to read all files from a selected folder.

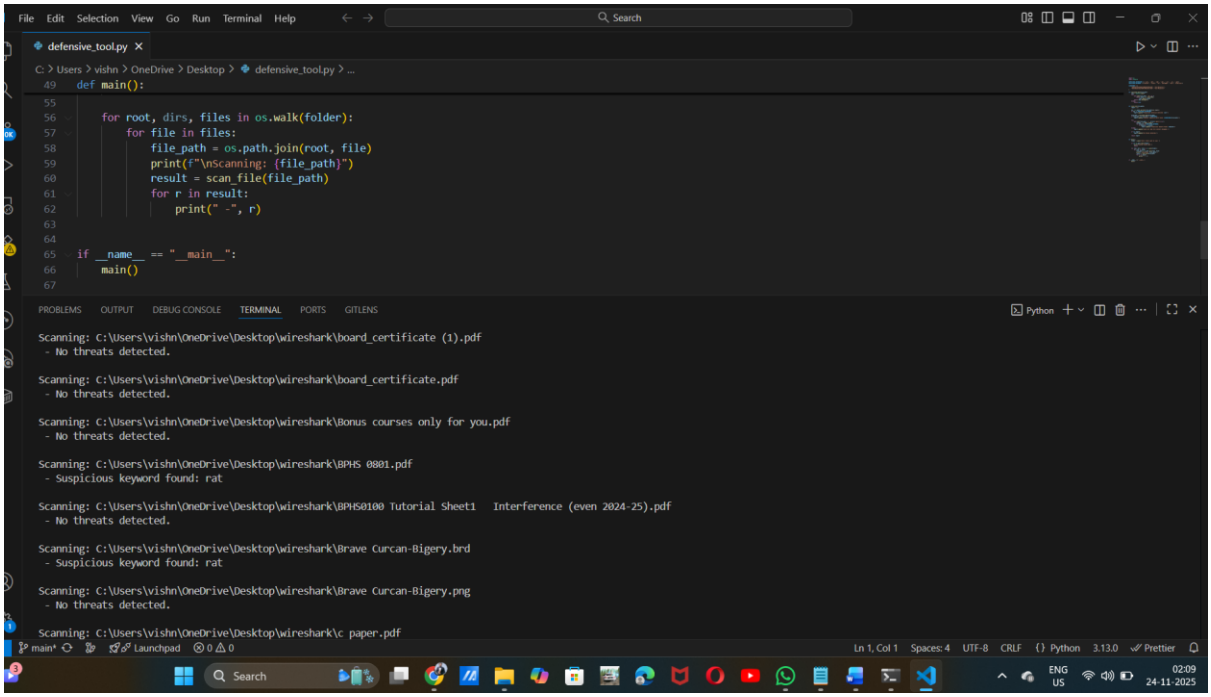
3. I added checks for suspicious extensions like .exe, .bat, .apk, etc.

4. I added keyword checking for words like “malware”, “rat”, “trojan”.

5. I ran the tool by entering a folder path in the terminal.
6. The tool scanned each file and displayed results.
7. I saved the final output for my report.

5. Output





The output shows the result of scanning multiple files using the defensive tool.

6. Conclusion

I completed the defensive scanning tool successfully.
This task helped me understand basic malware detection, file scanning, and simple defensive techniques in cybersecurity.