

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

```
File Edit View

import os
import hashlib

SUSPICIOUS_EXTENSIONS = ['.exe', '.bat', '.cmd', '.vbs', '.scr', '.js', '.apk']
SUSPICIOUS_KEYWORDS = ['malware', 'trojan', 'rat', 'keylogger', 'hack', 'suspicious']

SIGNATURES = {
    "e99a18c428cb38d5f260853678922e03": "Test-Malware-1",
    "5d41402abc4b2a76b9719d911017c592": "Test-Malware-2"
}

def calculate_hash(file_path):
    sha1 = hashlib.sha1()
    try:
        with open(file_path, 'rb') as f:
            while chunk := f.read(4096):
                sha1.update(chunk)
        return sha1.hexdigest()
    except:
        return None

def scan_file(file_path):
    report = []

    ext = os.path.splitext(file_path)[1].lower()
    if ext in SUSPICIOUS_EXTENSIONS:
        report.append(f"Suspicious extension detected: {ext}")

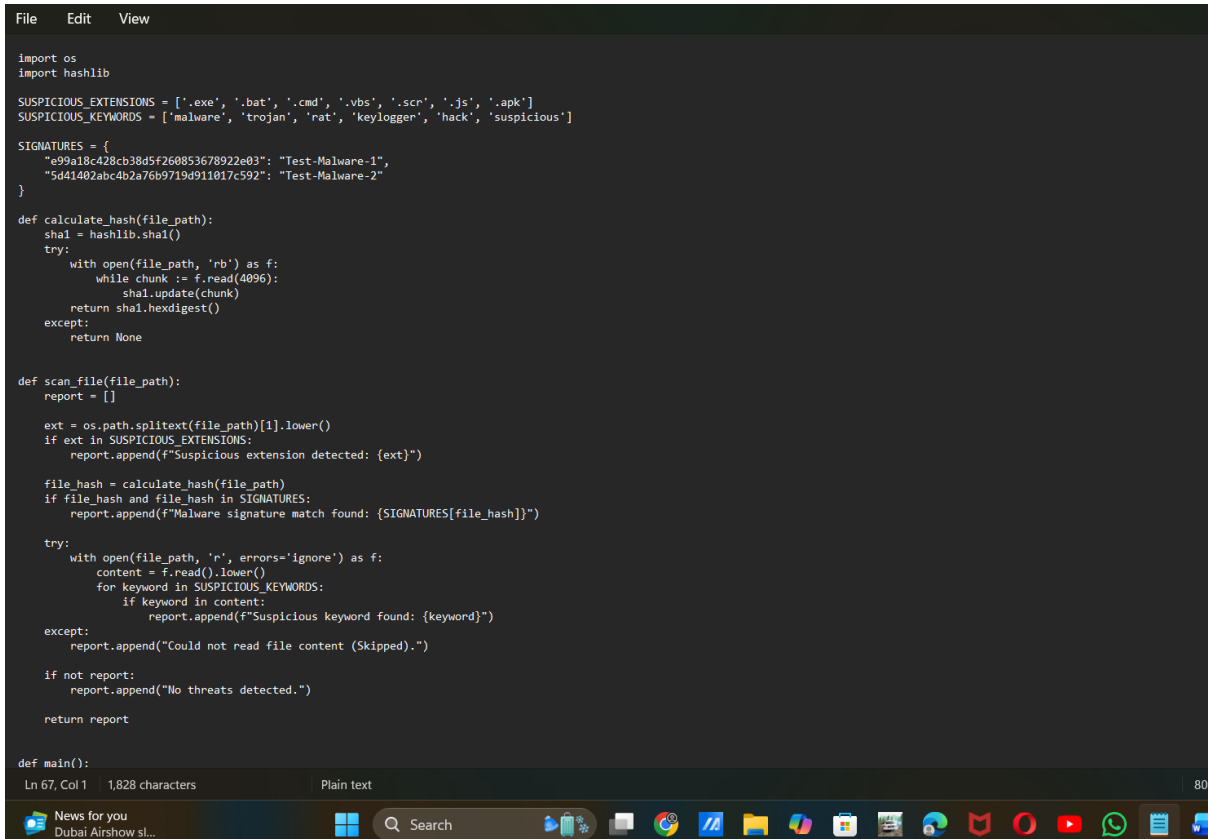
    file_hash = calculate_hash(file_path)
    if file_hash and file_hash in SIGNATURES:
        report.append(f"Malware signature match found: {SIGNATURES[file_hash]}")

    try:
        with open(file_path, 'r', errors='ignore') as f:
            content = f.read().lower()
            for keyword in SUSPICIOUS_KEYWORDS:
                if keyword in content:
                    report.append(f"Suspicious keyword found: {keyword}")
    except:
        report.append("Could not read file content (Skipped).")

    if not report:
        report.append("No threats detected.")

    return report

def main():
    Ln 67, Col 1 1,828 characters Plain text 80
```



The image shows a Windows 11 desktop environment. In the foreground, a Visual Studio Code (VS Code) editor window is open, displaying a Python script named `defensive_tool.py`. The script is a directory scanner that iterates through files in a specified folder, checks for threats, and prints the results. The code is as follows:

```
def main():  
    for root, dirs, files in os.walk(folder):  
        for file in files:  
            file_path = os.path.join(root, file)  
            print(f"\nScanning: {file_path}")  
            result = scan_file(file_path)  
            for r in result:  
                print(" -", r)  
  
if __name__ == "__main__":  
    main()
```

The terminal window at the bottom of the VS Code editor shows the output of the script. It scans several files on the desktop, including PDFs and images. The output is as follows:

```
Scanning: C:\Users\vishn\OneDrive\Desktop\wireshark\board_certificate (1).pdf  
- No threats detected.  
  
Scanning: C:\Users\vishn\OneDrive\Desktop\wireshark\board_certificate.pdf  
- No threats detected.  
  
Scanning: C:\Users\vishn\OneDrive\Desktop\wireshark\Bonus courses only for you.pdf  
- No threats detected.  
  
Scanning: C:\Users\vishn\OneDrive\Desktop\wireshark\BPHS 0801.pdf  
- Suspicious keyword found: rat  
  
Scanning: C:\Users\vishn\OneDrive\Desktop\wireshark\BPHS0100 Tutorial Sheet1 Interference (even 2024-25).pdf  
- No threats detected.  
  
Scanning: C:\Users\vishn\OneDrive\Desktop\wireshark\Brave Curcan-Bigery.brd  
- Suspicious keyword found: rat  
  
Scanning: C:\Users\vishn\OneDrive\Desktop\wireshark\Brave Curcan-Bigery.png  
- No threats detected.  
  
Scanning: C:\Users\vishn\OneDrive\Desktop\wireshark\c paper.pdf
```

The taskbar at the bottom of the screen shows various application icons, including the Start menu, Search, File Explorer, and several other open applications. The system clock in the bottom right corner indicates the time is 02:09 on 24-11-2023.