Final Project

📑 Project Documentation – File Integrity Monitoring (FIM) using PowerShell

---

1. Project Title

File Integrity Monitoring (FIM) using PowerShell – A Purple Team Simulation

---

2. Introduction

This project implements a File Integrity Monitoring system to detect and log file changes in real time. FIM plays a crucial role in cybersecurity by ensuring that files are not altered, deleted, or tampered with by unauthorized users.

---

3. Objectives

- To monitor file system activities such as Create, Modify, Rename, and Delete.
- To verify file integrity using SHA256 hashing.
- To log all detected activities with timestamp, username, and file path.
- To simulate both attacker actions (tampering files) and defender detection (logging changes).

---

4. Scope of the Project

- The project focuses on monitoring a specific folder (watched).
- It is implemented using PowerShell scripting.
- Logs are stored locally in fim_log.txt.

- The project demonstrates a Purple Team approach by showing both attack and defense perspectives.

---

5. Tools and Technologies Used

- PowerShell (scripting language).
- FileSystemWatcher (event-driven detection).
- SHA256 Hashing (integrity verification).
- Windows Operating System.

---

6. System Design / Methodology

- Create folder structure: watched, logs, watcher.ps1.
- Start watcher script in PowerShell.
- Perform file operations (create, modify, rename, delete).
- Watcher logs activities in real time.
- Hash polling ensures even silent modifications are detected.

---

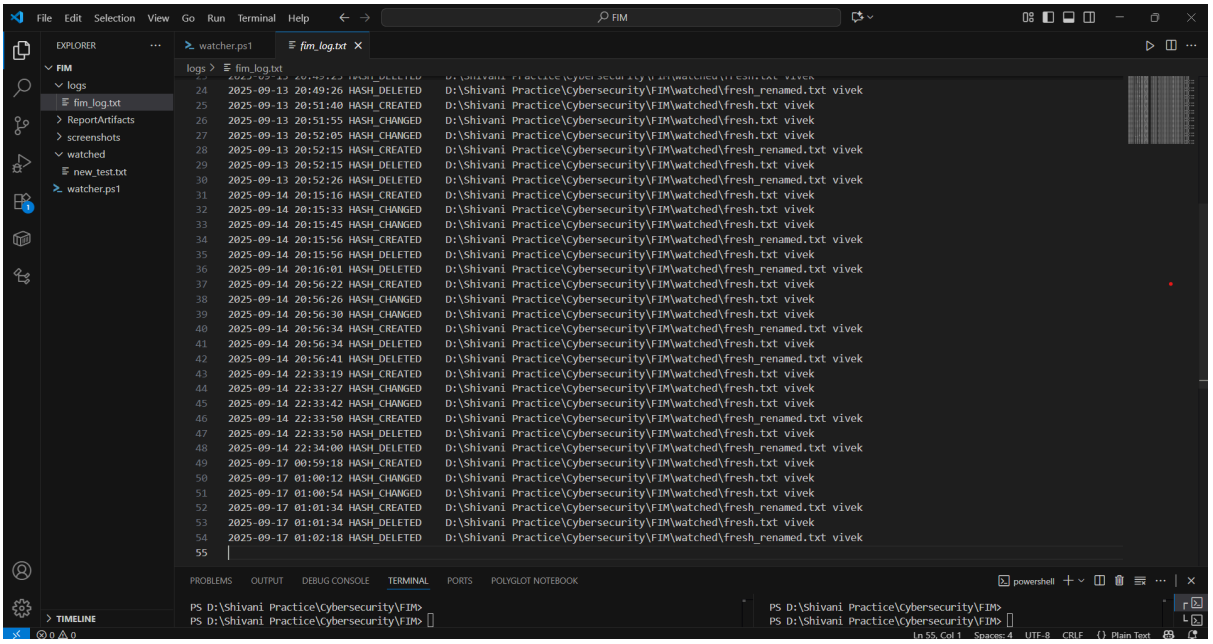
7. Implementation Steps

1. Run the watcher script.
2. Create a file in the watched folder → logs Created.
3. Modify the file → logs Hash Changed.
4. Rename the file → logs Renamed.
5. Delete the file → logs Deleted.
6. Verify events in fim_log.txt.

---

8. Results / Output

- Real-time detection of file activities.
- Log entries showing:



---

9. Use Cases / Applications

- Detecting unauthorized file modifications by insider threats.
- Identifying ransomware activity (mass file changes).
- Ensuring compliance with standards like PCI-DSS, HIPAA, ISO 27001.
- Auditing sensitive folders in enterprises.

---

10. Security Importance

- FIM is part of the CIA Triad → protects Integrity.
- Helps in digital forensics by providing tamper-proof logs.
- Acts as an early warning system for attacks.
