**Project Report on Log File Analyzer**

**1. Title Page**

Project Title: Log File Analyzer

Submitted by : Pallavi Gurame

internship : cyber security intern

Organization Name : internship at Elevate Labs

Date: 08/09/2025

**2. Abstract**

This project aims to develop a Log File Analyzer tool that processes system and application log files to detect suspicious activities such as malware, unauthorized access, phishing attempts, file tampering, and security breaches. The tool helps system administrators and SOC analysts to gain insights into security events, ensuring faster incident detection and response.

**3. Introduction**

Log files store records of events happening in computer systems, networks, or applications. Analyzing these logs manually is time-consuming and error-prone. The purpose of this project is to automate the analysis process using a Python-based tool that can extract, filter, and highlight suspicious activities from log files.

**Objectives:**

To collect and analyze system log files.

To detect anomalies and security threats from logs.

To generate structured output for visualization and reporting.

**Scope:**

This project can be used in small organizations, educational labs, or by SOC teams for learning and practicing log analysis.

**4. Literature Review**

Manual log analysis methods are inefficient.

Existing SIEM tools like Splunk, ELK Stack are powerful but costly.

Lightweight Python-based solutions provide learning and affordable alternatives.

**5. Methodology / System Design**

Technologies Used:

Language: Python

Libraries: Pandas, seaborn ,CSV, Matplotlib (for visualization)

Input: Log files (Windows Event Logs, Security logs, etc.)

Output: Structured CSV reports, suspicious activity detection

**Process Flow:**

Collect log files.

Parse and filter logs.

Identify suspicious keywords (e.g., failed login, error, access denied).

Export results to CSV.

Visualize results with graphs.

**6. Implementation / Work Done**

Developed a Python script to read and parse logs.

Converted logs into CSV format for structured analysis.

Applied filtering rules to highlight abnormal events.

Created visual charts to show frequency of events.

**7. Results and Discussion**

Successfully analyzed sample Windows/Linux log files.

Detected suspicious login attempts and errors.

Output shown in CSV format with event details (timestamp, user, action, status).

Graphs plotted for event frequency and type distribution.

**8. Conclusion and Future Work**

Conclusion:

The Log File Analyzer project provides an efficient way to process and analyze logs for security monitoring. It reduces manual effort and helps in faster incident response.

**Future Enhancements:**

Integration with a database for long-term log storage.

Real-time log monitoring with alerts.

Adding Machine Learning for anomaly detection.

Integration with SIEM dashboards.

**9. References**

“Python for Cybersecurity” by Packt Publishing.

Splunk and ELK Stack Documentation.

Online tutorials and official Python documentation.

**10) Appendix**

Python code (script).

Sample log files.

CSV output screenshots.

Visualization graphs