Log Analysis Assignment

Overview

This lab assignment focuses on the practical application of log analysis to identify security issues within a fictional organization. You will analyze the provided sample security logs and develop a basic report with findings and recommendations.

Learning Objectives

By completing this lab, you will be able to:

- Identify potential security incidents or anomalies from log data.
- Propose basic remediation steps for identified issues.

Scenario

Global Tech, a mid-sized financial technology company, has collected security logs from its SIEM system. Your task is to analyze a subset of these logs to identify any critical security events or patterns.

Tasks

1. Review the provided sample security log files.
2. Identify at least two potential security incidents, anomalies, or operational inefficiencies from the log data.
3. For each identified issue, provide a brief explanation of why it is a concern.
4. Suggest a simple, actionable remediation step for each identified issue.

Deliverables

- A short report (1-2 pages) in pdf format detailing your findings, explanations, and proposed remediation steps.

Appendix: Sample Security Log Data

Sample log files. These will include simplified versions of:

- Failed Authentication Attempts
- Vulnerability Scan Results
- Security Incidents