Log Analysis Report

Introduction:
Log analysis is the process of reviewing and examining system-generated logs to detect security threats, troubleshoot errors, monitor system performance, and maintain overall system health. Logs are generated by operating systems, applications, servers, and network devices. Proper log analysis helps organizations identify suspicious activities, system failures, and unauthorized access.

Objectives of Log Analysis:

1. Monitor system activities and user behavior
2. Detect unauthorized access or attacks
3. Troubleshoot system and application errors
4. Improve system performance and reliability
5. Maintain security compliance and auditing

Types of Logs:

1. System Logs – Record operating system events and activities
2. Application Logs – Track application-level errors and operations
3. Security Logs – Monitor login attempts and security events
4. Network Logs – Capture network traffic and connections
5. Server Logs – Record server requests and responses

Short Log Analysis Example:
During the analysis of system logs, multiple failed login attempts were detected from an unknown IP address. This activity indicates a possible brute-force attack. The system administrator blocked the suspicious IP and updated firewall rules to prevent further unauthorized access.

Detailed Log Analysis:
The log files were collected from system, application, and security sources. After reviewing the logs, several events were identified including repeated login failures, unusual system shutdowns, and high CPU usage during non-working hours. Security logs revealed unauthorized access attempts using invalid credentials, indicating potential malicious activity.

Network logs showed abnormal traffic from external sources attempting to access restricted ports. Immediate actions were taken including enabling firewall protection, disabling unused services, and updating system passwords. Continuous monitoring and automated log management tools were recommended to improve future security and performance.

This log analysis demonstrates the importance of monitoring logs regularly to detect threats early and maintain system integrity.

Conclusion:
Log analysis is an essential part of cyber security and system administration. It helps in identifying errors, detecting attacks, and improving performance. Regular monitoring and proper log

management ensure system safety and reliability.