Name : Patel Dhruv Nirmalkumar
Email : dhruvpatel.00700@gmail.com
Phone : 9426176903
Task : 12

Log Analysis Report

Summary

This report presents the results of a log analysis exercise focused on identifying potential security incidents in authentication logs. The primary objective was to detect suspicious login activity, analyze failed authentication attempts, identify anomalies, and correlate events across multiple log sources.

The analysis revealed a simulated brute-force attack targeting the root user from the IP address 185.12.34.56, along with multiple failed login attempts using invalid usernames. The report also briefly explains core SIEM concepts and outlines example alerting rules.

Methodology

The log analysis was conducted in a sandboxed Linux environment. Since real-time production logs were unavailable, synthetic log files were created to simulate realistic authentication and system events.

The following steps were performed:

1. **Log Generation**
    - A Python script (generate_logs.py) was used to generate synthetic auth.log and syslog files.
    - The auth.log file included a simulated SSH brute-force attack targeting the root account from IP 185.12.34.56.
2. **Log Inspection**
    - Initial inspection of auth.log was performed to understand its format and event structure.
3. **Authentication Log Analysis**
    - Linux command-line tools such as grep, awk, sort, and uniq -c were used to:
        - Count failed login attempts
        - Identify source IP addresses
        - Identify targeted usernames
        - Detect invalid user attempts

4. **Anomaly Detection and Event Correlation**
    - Manual correlation was performed between auth.log and syslog entries.
    - Events associated with the most suspicious IP address were analyzed across both logs.
5. **SIEM Basics and Alerting**
    - SIEM fundamentals were reviewed.
    - Common alert rules for detecting SSH brute-force attacks were studied.
6. **Documentation**
    - All findings and responses to the guiding questions were documented in this report.

Findings

Authentication Attempts Overview

Analysis of the auth.log file showed a high number of failed authentication attempts.

Failed Login Attempts by Source IP

Source IP Address	Failed Attempts
185.12.34.56	42
45.33.22.11	18
192.168.1.10	16
172.16.0.20	12
10.0.0.5	7

Failed Login Attempts by Username

Target Username	Failed Attempts
root	43
db_admin	15
user1	12
guest	9
webmaster	8
admin	8

Anomalous Activity: Brute-Force Attack

The IP address 185.12.34.56 generated the highest number of failed login attempts, totaling **42 attempts**.

Key observations:

- Most attempts targeted the root user.
- Multiple consecutive Failed password entries appeared within a short time window.
- This behavior strongly indicates a **brute-force SSH attack**.
- Several Invalid user attempts were also observed, including:
    - test
    - oracle
    - guest123

These attempts suggest reconnaissance activity using commonly guessed or default usernames.

Event Correlation

Correlation between auth.log and syslog revealed consistent authentication failure messages for the same timestamps and source IP.

Key correlated events:

- auth.log entries showed repeated Failed password messages.
- syslog entries recorded:
    - pam_unix(sshd:auth): authentication failure
- Both logs referenced the same IP address (185.12.34.56) and time ranges.

This confirms that the authentication failures were captured across multiple logging mechanisms, strengthening confidence in the detection.

Recommendations

Based on the analysis, the following security improvements are recommended:

1. **Account Lockout Policies**
    - Lock accounts temporarily after a defined number of failed login attempts.
2. **Strong Password Enforcement**
    - Enforce complex, unique passwords.
    - Regularly rotate credentials for privileged accounts.
3. **Multi-Factor Authentication (MFA)**
    - Require MFA for all critical and administrative accounts.
4. **Restrict SSH Access**
    - Limit SSH access to trusted IP ranges.
    - Disable password-based authentication where possible.
    - Use SSH key-based authentication instead.
5. **Deploy a SIEM Solution**
    - Centralize log collection.
    - Enable automated detection and correlation.
    - Support real-time alerting and investigation.
6. **Configure Alert Rules**
    - Trigger alerts for:
        - Multiple failed login attempts from a single IP
        - Login attempts to privileged accounts
        - Successful logins following multiple failures
7. **Regular Log Review**
    - Perform scheduled manual or automated log reviews to detect patterns and anomalies.

Conclusion

This log analysis exercise successfully demonstrated how authentication logs can be used to detect security incidents such as brute-force attacks. The simulated attack on the root account highlighted the importance of continuous monitoring, log correlation, and proactive alerting.

By implementing the recommended controls and deploying a SIEM solution, organizations can significantly improve their ability to detect, respond to, and prevent authentication-based attacks.