**Incident Response & Digital Forensics**

**Assignment 2 : Analysis of Suspicious Login Attempts from /var/log/auth.log**

**Introduction**

This assignment presents an analysis of system authentication logs captured in the /var/log/auth.log file to identify any suspicious login attempts or security-related events. The purpose is to detect unauthorized access, anomalous login activities, and related authentication issues to improve system security monitoring.

**Scope and Objective**

The analysis focuses on login events on the system dated 15th October 2025, observed from the provided log excerpt. The objective is to extract timestamps and associated IP addresses (where available) of suspicious login attempts and document any notable findings, including successful root access, failed attempts, and system errors.

**Tools and Environment**

* Linux system with access to /var/log/auth.log
* Command-line utilities such as cat, grep, and awk used to extract relevant log entries
* Manual log inspection complementing command-line parsing

**Methodology**

1. Accessed the authentication log file at /var/log/auth.log.
2. Parsed log entries for key terms indicative of login activity, including "login", "session opened", "failed password", and "root login".
3. Extracted and tabulated timestamps and relevant event information such as usernames, IP addresses (if present), and device terminals.
4. Analyzed system messages for errors affecting authentication processes.
5. Evaluated the data for signs of repeated failed attempts, unauthorized logins, and irregular patterns.

**Findings:**

| **Timestamp (UTC)** | **Event Description** | **User** | **IP Address** | **Notes** |
| --- | --- | --- | --- | --- |
| 2025-10-15T08:21:40.314090 | PAM module pam\_lastlog.so missing | N/A | N/A | PAM module missing; potential logging impact |
| 2025-10-15T08:21:41.052938 | Session opened for user root (UID=0) | root | N/A | Successful root login; high privilege |
| 2025-10-15T08:21:41.493088 | Root login on terminal /dev/pts/1 | root | N/A | Interactive root login via terminal |
| 2025-10-15T08:25:00.421577 | Cron session started for root user | root | N/A | Scheduled task running |
| 2025-10-15T08:25:00.428372 | Cron session closed for root user | root | N/A | Scheduled task completed |

* No failed login attempts or external IP addresses were present in the provided log entries.
* Missing PAM module pam\_lastlog.so indicates some incomplete PAM configuration which could impact log completeness.
* Root user activity is documented with explicit session open logs at terminal device /dev/pts/1.
* Cron job execution under root proceeded normally without anomalies.

**Analysis and Interpretation**

The log entries indicate legitimate and authorized root user activity within the system, without any observed suspicious or malicious login attempts in the given excerpt. The absence of failed password messages or abnormal IP addresses suggests no evident external brute force attack or unauthorized login attempt at this time.

However, the missing PAM module error should be addressed as it may limit session logging and auditing capabilities, potentially reducing forensic visibility.

**Conclusion**

The analysis of the /var/log/auth.log entries from 15th October 2025 reveals expected system behavior with successful root logins and no detected suspicious login attempts or security incidents within the observed timeframe. Addressing the missing PAM module and continuing vigilant log monitoring is advised to uphold system security.

