**SOC Log Analysis & Alerting Project**  
Author: Hanan Fathima K  
Date: 21-07-2025

**1. Introduction**

The purpose of this project is to simulate the role of a SOC (Security Operations Center) analyst by analyzing sample Windows Event Logs and Linux authentication logs to detect suspicious activity. The goal is to identify possible security threats such as brute-force login attempts, privilege escalation, and password changes, and then assign severity levels to these events using a structured approach. Additionally, all findings are mapped to the MITRE ATT&CK framework to align with real-world threat detection methodologies.

**2. Suspicious Findings**

**Windows Event Log:**

* Event ID 4794: Attempt to set the Directory Services Restore Mode (DSRM) administrator password (Medium Severity).

**Linux Authentication Log:**

* Multiple failed SSH login attempts for an invalid user (192.168.1.10).
* Failed root login from external IP 203.0.113.5.
* Privileged command executed by user 'mary' via sudo (nano /etc/hosts).

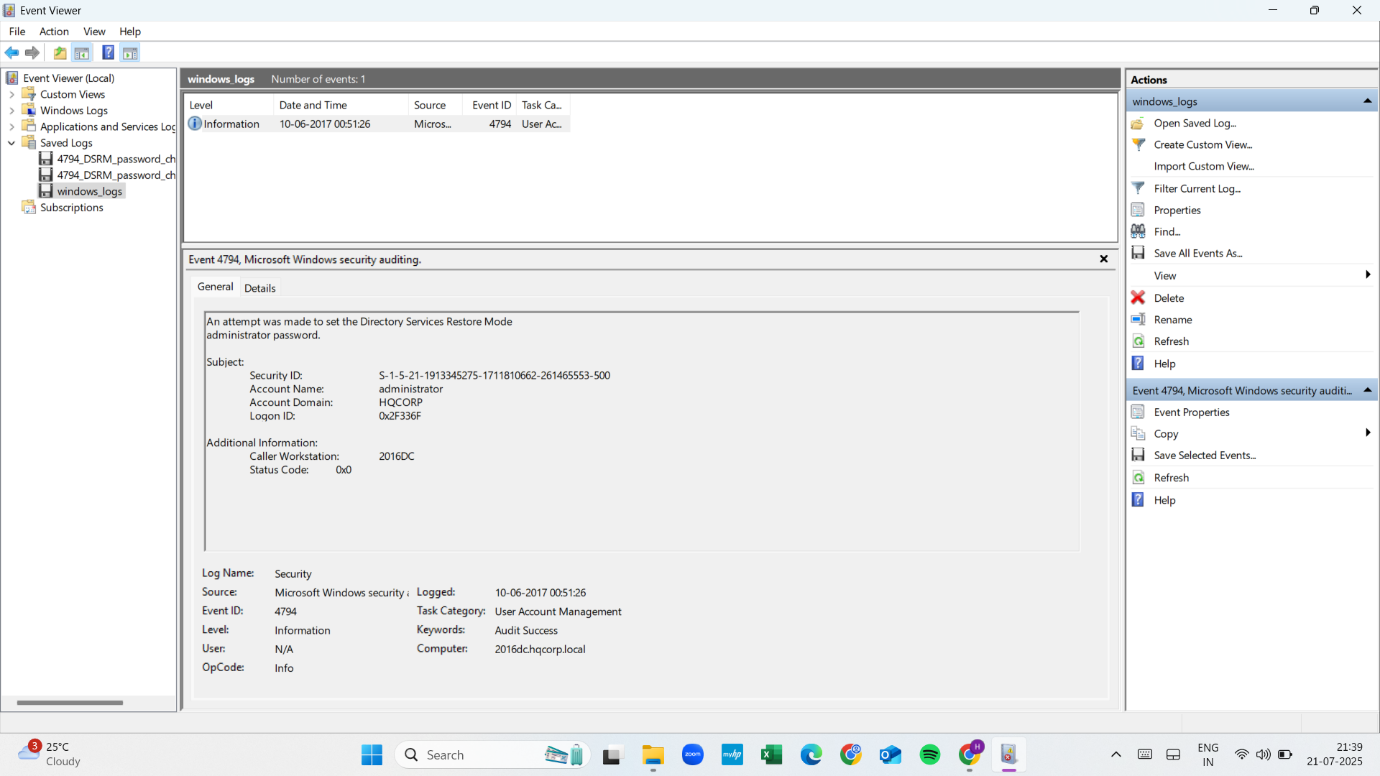
**3. Severity Analysis**

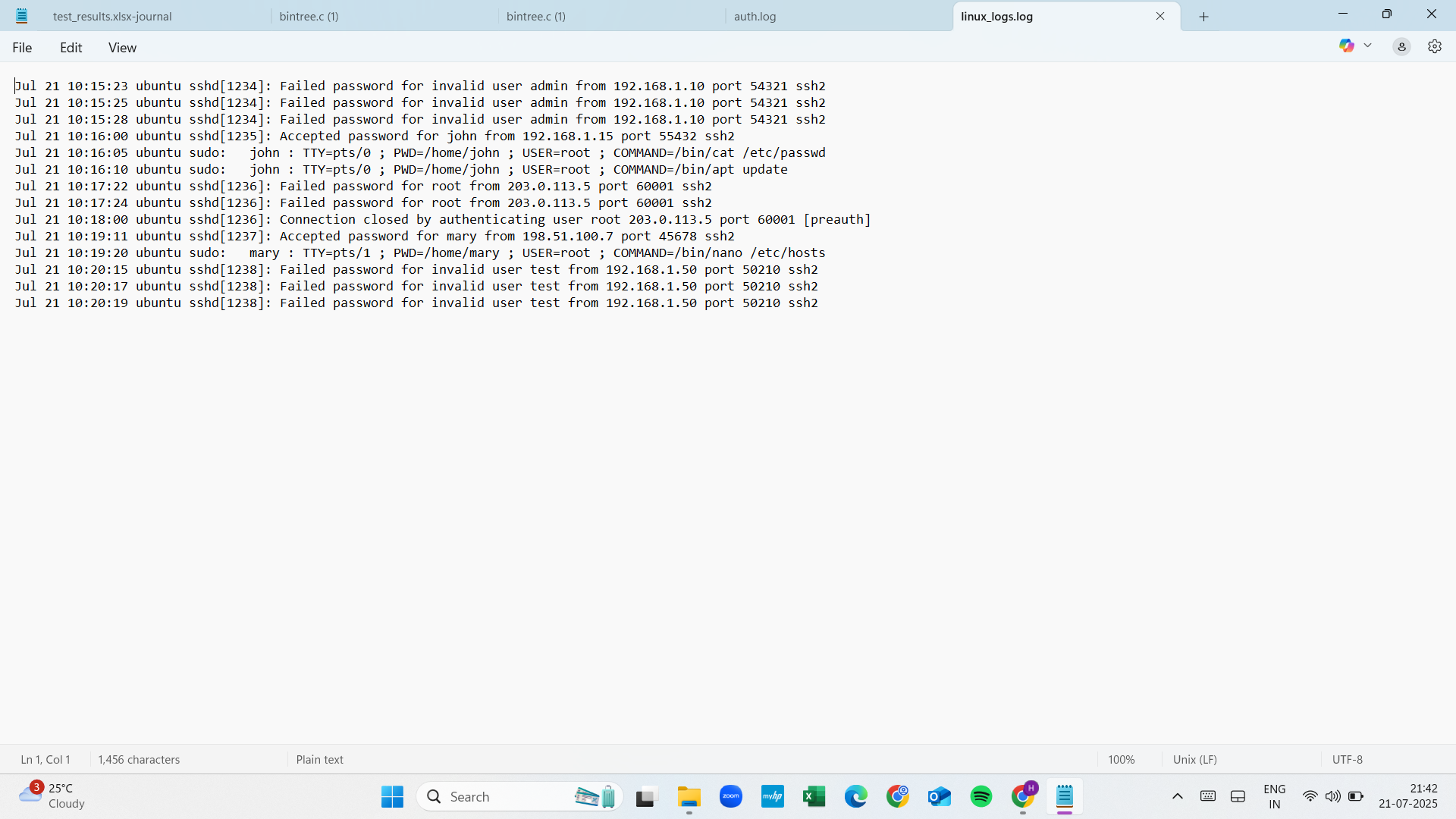
| **#** | **Platform** | **Evidence (Log Snippet / Event ID)** | **What It Indicates** | **Severity** | **Notes / Action** |
| --- | --- | --- | --- | --- | --- |
| 1 | Windows | Event ID 4794 – Attempt to set DSRM admin password | Possible privilege escalation or persistence attempt | Medium | Investigate if expected. |
| 2 | Linux | 3× Failed SSH logins for invalid user admin from 192.168.1.10 | Brute-force attempt | Medium | Check firewall and block source IP. |
| 3 | Linux | 2× Failed SSH logins for root from 203.0.113.5 | Root account targeted from external IP | High | Block IP and investigate further. |
| 4 | Linux | Sudo command by mary editing /etc/hosts | Potential configuration tampering | Medium | Verify if authorized. |

**4. MITRE ATT&CK Mapping**

| **#** | **Event** | **MITRE Tactic** | **MITRE Technique (ID)** | **Why It Matches** |
| --- | --- | --- | --- | --- |
| 1 | Windows Event ID 4794 – Attempt to set DSRM admin password | Persistence / Privilege Escalation | T1098 – Account Manipulation | Attackers often change passwords for persistence. |
| 2 | Linux – Multiple failed SSH logins (192.168.1.10) | Initial Access | T1110 – Brute Force | Repeated password guessing matches brute-force attacks. |
| 3 | Linux – Failed root login from 203.0.113.5 | Initial Access | T1078 – Valid Accounts | Attempt to gain access via root credentials. |
| 4 | Linux – mary used sudo to edit /etc/hosts | Privilege Escalation / Defense Evasion | T1548 – Abuse Elevation Control Mechanism | Using sudo for elevated changes. |

**5. Screenshots**





**6. Conclusion**

The log analysis successfully identified suspicious activities across Windows and Linux environments, including brute-force login attempts, failed root logins, and administrative password changes. Severity levels were assigned to each event, and each finding was mapped to a relevant MITRE ATT&CK technique to replicate real-world SOC analysis processes. This project demonstrates practical skills in log analysis, threat detection, and incident documentation.