Security Alert Analysis Report

Session ID:	c5a46c65-44dc-42...
Alert ID:	5aea9541-1069-463d-9851-ec021784f7b9
Created:	2025-11-04T05:41:41.171759
Messages:	4
Playbooks Used:	0

Alert Summary

I'll provide a concise alert summary based on the security alert details. Let me search for the most relevant security playbook for this incident.
Let me try searching with more specific terms related to credential access:
Let me check if there's a more specific credential access playbook:
Based on the search results, I can now provide a concise alert summary:

1. WHAT HAPPENED (2 lines maximum):
Multiple consecutive login attempts were detected targeting a local Linux user account from a single process, indicating a potential brute force attack to gain unauthorized access.

2. IMMEDIATE MITIGATION REQUIRED:
Answer: YES

3. RECOMMENDED PLAYBOOK:
Brute_Force_Protection_Playbook

Key Recommendations

1. Multiple consecutive login attempts

2. Targeting a local Linux user account

3. Coming from a single process

4. Occurring within a short time interval

5. Authentication logs (such as /var/log/auth.log or /var/log/secure) for:

6. Multiple failed login attempts

7. Login attempts targeting the same or multiple user accounts

8. Login attempts occurring in rapid succession

9. Process information:

10. The alert mentions login attempts executed by a single process

Recommended Response Playbooks

I'll help you identify the most appropriate security playbooks for this incident. Let me search for relevant playbooks based on the alert details.
Let me also check for more specific credential access playbooks:
Based on the analysis of the security alert involving multiple consecutive login attempts on a Linux user account, I recommend following the Brute Force Protection Playbook with the following key response steps:

Immediate containment is critical. The SOC analyst should first isolate the affected Linux account by temporarily disabling it or implementing strict access controls. Utilize the Brute Force Protection Playbook to conduct a thorough log analysis, focusing on identifying the source IP addresses, examining the frequency and pattern of login attempts, and determining if any successful breaches occurred. Pay special attention to log events that indicate potential credential stuffing or unauthorized access attempts.

For long-term mitigation, implement multi-layered security controls. This includes enforcing multi-factor authentication (MFA) for the compromised account, reviewing and tightening authentication thresholds, and conducting a comprehensive password audit. The playbook recommends reducing allowed connection limits, potentially blocking the source IP addresses, and implementing additional monitoring for suspicious login activities. Consider conducting a broader security review to ensure no lateral movement or additional compromises have occurred as a result of these repeated login attempts.

Conversation Highlights

User:
I need your help analyzing this security alert. Please provide analysis and recommendations based on the rule-to-text summary and analyst report provided in your system context. Use the search_playbook_knowledge or search_security_playbooks_by_topic tools to find relevant response procedures from our security playbooks.

User:
Is there any relevant IoC in the alert?

Assistant:
Looking at the alert data, I need to check if there are any Indicators of Compromise (IoCs) mentioned. Let me analyze the raw alert data for you.

Based on my review of the alert data, I don't see specific IoCs like IP addresses, file hashes, or malicious domains explicitly listed in the alert. The "pre_extracted_iocs" section in the alert data shows empty arrays for processes, user accounts, and ports:

```json
"pre_extracted_iocs": {
"processes": [],
"user_accounts": [],
"ports": []
}
``...
```