

Security Alert Analysis Report

Session ID:	29184e0b-cd29-45...
Alert ID:	5aea9541-1069-463d-9851-ec021784f7b9
Created:	2025-11-10T23:13:00.391535
Messages:	6
Playbooks Used:	0

Alert Summary

1. WHAT HAPPENED (2 lines maximum):

A single process executed multiple consecutive login attempts against a local Linux user account within a short timeframe, indicating a potential credential brute force attack. 8 processes and 1 targeted user account have been identified as indicators of compromise.

2. IMMEDIATE MITIGATION REQUIRED:

YES - Active brute force attempts require immediate action to prevent unauthorized account access.

3. RECOMMENDED PLAYBOOK:

Brute Force Protection Playbook

Key Recommendations

1. `su` (switch user - comando legítimo mas usado de forma suspeita)
2. `targeting`
3. `identified`
4. `execution`
5. **Usuário:** `root`
6. Esta é a conta com privilégios máximos no sistema Linux, tornando o ataque particularmente crítico
7. **Múltiplas tentativas consecutivas de login** executadas por um único processo
8. **Timeframe curto** (maxspan de 1 segundo configurado na regra)
9. **Tipo de ataque:** Brute Force de credenciais
10. **Sistema Operacional:** Linux

Recommended Response Playbooks

Security Playbook Recommendations

Based on the alert analysis, the SOC analyst should immediately follow the **Brute Force Protection Playbook** as the primary response procedure. This incident involves multiple consecutive login attempts against a local Linux user account (8 suspicious processes targeting 1 user account), which is a clear indicator of a credential brute force attack. The playbook recommends first **investigating the attack scope** by examining log messages to identify the source IPs, autonomous system numbers, or countries involved in the attack, then **implementing immediate containment measures** including blocking malicious IPs at the firewall/reverse proxy level, tightening brute force thresholds, and disabling unused authentication endpoints. Additionally, enforce multi-factor authentication (MFA) for the compromised account and reset credentials for the targeted user account immediately.

As a secondary consideration, consult the **Root Access Playbook** for containment procedures, particularly if there's any indication that the targeted account has elevated privileges or if any login attempts were successful. This playbook provides guidance on identifying systems at risk, systems to be taken offline due to compromise, accounts that need to be locked out, and unauthorized tools used in the attack. The analyst should document all compromised user accounts, identify any successful authentication events from the 8 suspicious processes, verify whether any lateral movement occurred, and assess the impact on IT services. Priority actions include isolating affected systems, forcing password resets for impacted accounts, reviewing authentication logs for the timeframe of the attack, and conducting forensic analysis to determine if any data exfiltration or persistence mechanisms were established.

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:

Quais os indicadores de comprometimento(iocs) encontrados?

Assistant:

Com base na análise do alerta, aqui estão os **Indicadores de Comprometimento (IoCs)** identificados:

IoCs Identificados:

1. Processos Suspeitos (8 processos)

Os seguintes processos foram identificados executando tentativas de login consecutivas:

- `su` (switch user - comando legítimo mas usado de forma suspeita)
- `targeting`
- `identified`
- `timeout`
- `event`
- `names`
- `where`
- `execution`
- `of`

2. Conta de Usuário Alvo (1 usuário)

- **Usuário:** `root`
- Esta é...

User:

Resuma as recomendações imediatas

Assistant:

Vou buscar as recomendações imediatas do playbook de proteção contra Brute Force:

RESUMO - RECOMENDAÇÕES IMEDIATAS

Com base no **Brute Force Protection Playbook**, aqui estão as ações prioritárias:

CONTENÇÃO IMEDIATA:

1. **Bloquear IPs Suspeitos**

- Identificar e bloquear os IPs de origem do ataque
- Usar firewall de aplicação web (WAF) ou listas de controle de acesso

2. **Proteger a Conta Root Comprometida**

- Forçar MFA (autenticação multifator) para a conta roo...

