

Security Alert Analysis Report

Session ID:	13c6121d-38e9-48...
Alert ID:	*
Created:	2025-11-04T04:36:09.272862
Messages:	6
Playbooks Used:	0

Alert Summary

I'll help you find the most relevant security playbook for this brute force alert. Let me search for appropriate playbooks based on the alert details.

Let me search for more specific information about brute force playbooks:

Based on the search results, I can now provide a focused response:

****1. WHAT HAPPENED (2 lines maximum):****

Brute force attack detected with multiple login attempts, indicated by 1 suspicious domain, 1 URL, and 3 ambiguous tokens flagged as potential indicators of compromise.

****2. IMMEDIATE MITIGATION REQUIRED:****

YES

****3. RECOMMENDED PLAYBOOK:****

Brute Force Protection Playbook

Key Recommendations

1. Host information:
2. Hostname: "security-lab"
3. IP addresses: 172.31.8.207, fe80::594f:a856:4c91:6231, fe80::fc63:68ff:feab:b3fb
4. MAC addresses: 02-06-F0-C1-E5-A3, FE-63-68-AB-B3-FB
5. Host ID: ec2205f0796b81eb20be635feb26bd23
6. Alert pattern:
7. 166 log entries in a 1-minute period (exceeding the threshold of 75)
8. This high volume of logs in a short timeframe is consistent with brute force attack patterns
9. Reputation: Clean
10. Location: San Francisco, United States

Recommended Response Playbooks

I'll help you find the most appropriate security playbooks for this brute force attack scenario. Let me search for relevant playbooks and response procedures.

Let me also search for specific playbook knowledge about brute force response:

Based on the analysis of the brute force attack alert, I recommend following a comprehensive incident response procedure focusing on containment, investigation, and mitigation.

The primary playbook to follow is the "Brute Force Protection Playbook", which outlines critical steps for addressing this type of security incident. The immediate response should include: 1) Investigating the log events and identifying the scope of the attack, 2) Analyzing the suspicious domain, URL, and the three ambiguous tokens flagged as potential indicators of compromise, and 3) Implementing immediate containment measures. Key actions include tightening authentication thresholds, blocking the source IP (172.31.8.207), and reviewing access logs for any successful breaches.

For long-term mitigation, the SOC analyst should: 1) Enable additional security controls like CAPTCHA, multi-factor authentication, and potentially breached password detection, 2) Review and modify web application firewall rules to block the attacking IP and similar sources, and 3) Conduct a thorough forensic analysis to understand the attack vector and prevent future attempts. The focus should be on quickly containing the threat while gathering sufficient evidence to prevent similar incidents and understand the attacker's methodology.

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:

what are the most important ioc's of this alert?

Assistant:

Based on the alert information provided, I need to analyze the Indicators of Compromise (IOCs) for this brute force attack alert. Let me review the data carefully.

Looking at the alert details, I notice there's mention of "1 suspicious domain, 1 URL, and 3 ambiguous tokens flagged as potential indicators of compromise" in the Rule-to-Text Summary. However, when examining the raw alert data, I don't see these specific IOCs listed in detail.

The most important IOCs I can identify from the raw al...

User:

Is the ip 172.31.8.207 flagged by any sources?

Assistant:

I'll check if the IP address 172.31.8.207 is flagged by any threat intelligence sources. Let me look up this IP address for you.

Based on the lookup results, the IP address 172.31.8.207 is not flagged as malicious:

- Reputation: Clean
- Location: San Francisco, United States
- ISP: Example ISP
- Threat Types: None detected
- Confidence Score: 85 (indicating high confidence in the "clean" assessment)

It's important to note that this IP address appears to be an internal IP address (172.31.x.x is...).