# Security Alert Analysis Report

| | |
|---|---|
| **Session ID:** | a3f558a2-2cd0-4e... |
| **Alert ID:** | db3e843e-1a24-4af0-ba69-d7b8b35624c8 |
| **Created:** | 2025-11-04T20:34:11.770750 |
| **Messages:** | 6 |
| **Playbooks Used:** | 0 |

## Alert Summary

**1. WHAT HAPPENED (2 lines maximum):**
Multiple consecutive login failures detected from a single external IP address targeting one user account within a short time window. This indicates a brute force credential access attempt using password guessing against the targeted user account.

**2. IMMEDIATE MITIGATION REQUIRED:**
NO - Low severity brute force attempt with failed login attempts. Monitor for successful compromise but no immediate damage occurring.

**3. RECOMMENDED PLAYBOOK:**
Brute Force Protection Playbook

## Key Recommendations

1. **Source IP Address: `186.194.168.172`**
2. This is the external IP address conducting the brute force attack
3. Multiple consecutive failed login attempts originated from this IP
4. **Recommended Action**: Block or monitor this IP address
5. **Targeted User Account: `testuser`**
6. This is the user account being targeted by the brute force attempt
7. **Recommended Action**: Reset credentials if compromise is suspected, enable MFA
8. **Process Name: `sshd`**
9. The SSH daemon process indicates this is an SSH brute force attack
10. Attack vector: SSH service (typically port 22)

# Recommended Response Playbooks

## Playbook Recommendation

Based on this alert, you should follow the **Brute Force Protection Playbook** for credential-based attacks. This is a low-severity incident since all login attempts failed and the source IP (186.194.168.172) shows no prior malicious activity (0% abuse confidence score). The primary response should focus on **monitoring and preventive hardening** rather than immediate containment.

**Recommended Response Steps:**
1. **Investigate and Document**: Query authentication logs to identify all failed login attempts from the source IP within the attack window. Document the targeted username, timestamp patterns, and attack duration. Check if this IP has attempted access to other user accounts or systems.
2. **Monitor for Escalation**: Set up enhanced monitoring for the targeted user account and source IP to detect any successful authentication or pattern changes. Look for follow-up credential stuffing attempts, password spraying across multiple accounts, or attempts from different source IPs targeting the same user.
3. **Implement Preventive Controls**: Consider notifying the targeted user to review their credentials and enable MFA if not already active. Evaluate tightening brute force protection thresholds, implementing CAPTCHA challenges, or enabling breached password detection. If attacks persist from this IP, implement temporary IP blocking or rate limiting. Given the clean IP reputation, avoid permanent blocking without additional suspicious activity.

No immediate escalation is required, but maintain vigilance for 24-48 hours to ensure this was an isolated incident rather than reconnaissance for a larger campaign.

# 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 IoCs in the alert?

**Assistant:**
Based on the alert data, here are the relevant **Indicators of Compromise (IoCs)** identified:

## Primary IoCs:

1. **Source IP Address: `186.194.168.172`**
- This is the external IP address conducting the brute force attack
- Multiple consecutive failed login attempts originated from this IP
- **Recommended Action**: Block or monitor this IP address

2. **Targeted User Account: `testuser`**
- This is the user account being targeted by the brute force attempt
- **Recommended Acti...

**User:**
is 186.194.168.172 a known malicious ip?

**Assistant:**
## IP Reputation Analysis for `186.194.168.172`

Based on the threat intelligence lookup, here's what I found:

### Good News:
- **Abuse Confidence Score: 0%** - This IP has no prior abuse reports
- **Total Reports: 0** - No previous malicious activity reports
- **Not Whitelisted**: Not a trusted IP
- **Not Tor Exit Node**: Not associated with Tor anonymization network

### Geolocation & Network Details:
- **Location**: United States
- **ISP**: Example ISP (Commercial)
- **Domain**: example.com
...

Generated by TG-Agent Cybersecurity LLM System on 2025-11-04 20:38:44