

Incident Title: SSH Brute Force Failed Password Threshold

Severity: Medium

Detection Source: Elastic SIEM rule (Elasticsearch query on filebeat-logs)

Affected Host: testing02

Time Window: January 20, 2026 ~11:17–11:18 (approx.)

The screenshot displays the Elastic SIEM interface. The top navigation bar shows 'Stack Management' and 'Rules'. The left sidebar contains 'Management' and 'Alerts and Insights'. The main content area shows an alert titled 'SSH Brute Force Failed Password Threshold' with a status of 'Recovered'. Below the alert, a table lists the alert details, including the alert name, status, start time, duration, and maintenance windows. The alert is triggered by a query matched on the 'filebeat-logs' index pattern. The alert history shows a single entry with a status of 'Recovered'.

The bottom section of the screenshot shows a search for 'message: "Failed password"' in the 'filebeat-logs' index pattern. The search results show 12 hits, with a breakdown by time window. The search results are displayed in a table with columns for '@timestamp', 'message', and 'agent.type'. The table shows three entries, all with a status of 'Failed password' and a message indicating an invalid user login attempt from 192.16.8.64.1 port 51632.

Observed Activity:

Multiple failed SSH authentication attempts targeting the user wronguser were observed on host testing02. A total of 12 failed login attempts occurred within a short time window, consistent with brute-force behavior.

Source:

Source IP identified from raw log messages in /var/log/auth.log (not parsed into structured fields by Filebeat).

Impact:

No successful authentication was observed. The attack did not result in account compromise.

Evidence:

- Multiple message: "Failed password" events in Kibana Discover
- Elastic rule triggered and later recovered once activity stopped

Recommended Response:

- Block offending source IP at firewall or network layer
- Enable fail2ban to rate-limit SSH authentication attempts
- Disable password-based SSH authentication and enforce key-based access
- Review SSH configuration and user access controls