

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 shows the Elasticsearch Stack Management interface. On the left, there's a sidebar with 'Management' selected, followed by sections for 'Ingest', 'Data', and 'Alerts and Insights'. Under 'Alerts and Insights', 'Rules' is selected. In the main area, a search bar at the top has 'Type Elasticsearch query' and 'SSH Brute Force – Failed Password Threshold' entered. Below the search bar, a card displays the rule status as 'Enabled' with 23 executions in the last 24 hours. It shows the 'Last response' was 'Succeeded' 32 seconds ago. A button to 'Notify when alerts generated' is present. To the right, under 'Definition', it says 'Rule type Elasticsearch query', 'Actions No actions', and 'Description Alert when matches are found during the latest query run.' It also shows 'Runs every 1 min' and 'Conditions 0 conditions'. Below this, the 'Alerts' tab is selected, showing one alert entry: 'query matched' with 'Status Recovered'. At the bottom, there's a search bar for 'Find apps, content, and more.' and a navigation bar with 'Discover', 'New', 'Open', 'Share', 'Alerts', 'Inspect', and 'Save' buttons.

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