

Incident Analysis Report on Security Monitoring | Oluwaseun Quadri

1. Executive Summary

On 13-02-2026, suspicious activity was detected through the ELK Stack SIEM platform. The logs indicated multiple failed authentication attempts originating from an external IP address targeting the Cowrie honeypot SSH service. The activity is consistent with a brute-force attack attempt.

2. Environment Overview

- SIEM Platform: ELK Stack (Elasticsearch, Logstash/Filebeat, Kibana)
- Log Source: Cowrie Honeypot (SSH)
- Monitoring Tool: Kibana Dashboard
- Deployment: Ubuntu Server (ELK) + Kali Linux (attacker simulation)

3. Detection Details

Detected Indicators:

- High number of failed login attempts
- Repeated authentication failures within short time window
- Single source IP performing multiple username/password attempts
- SSH protocol abuse

Example fields from logs:

- source.ip
- event.action: login_failed
- user.name
- @timestamp

4. Attack Analysis

Type of attack:

SSH Brute Force Attack

Observed behavior:

- Automated login attempts
- Sequential username/password combinations
- Rapid connection attempts

Likely tools:

- Hydra
- Medusa
- Custom brute-force script

5. Impact Assessment

Potential Risks:

- Credential compromise
- Unauthorized system access
- Lateral movement
- Data exfiltration

Severity Level:

Medium (since honeypot environment, no production impact)

6. Evidence Collected

- Kibana dashboard screenshots
- Log entries showing failed login attempts
- Source IP address correlation
- Time-based activity spike visualization

7. Recommended Mitigation

- Implement rate limiting

- Enable account lockout policy
- Deploy fail2ban
- Restrict SSH access via firewall
- Use key-based authentication instead of passwords

DELIVERABLE SCREENSHOTS

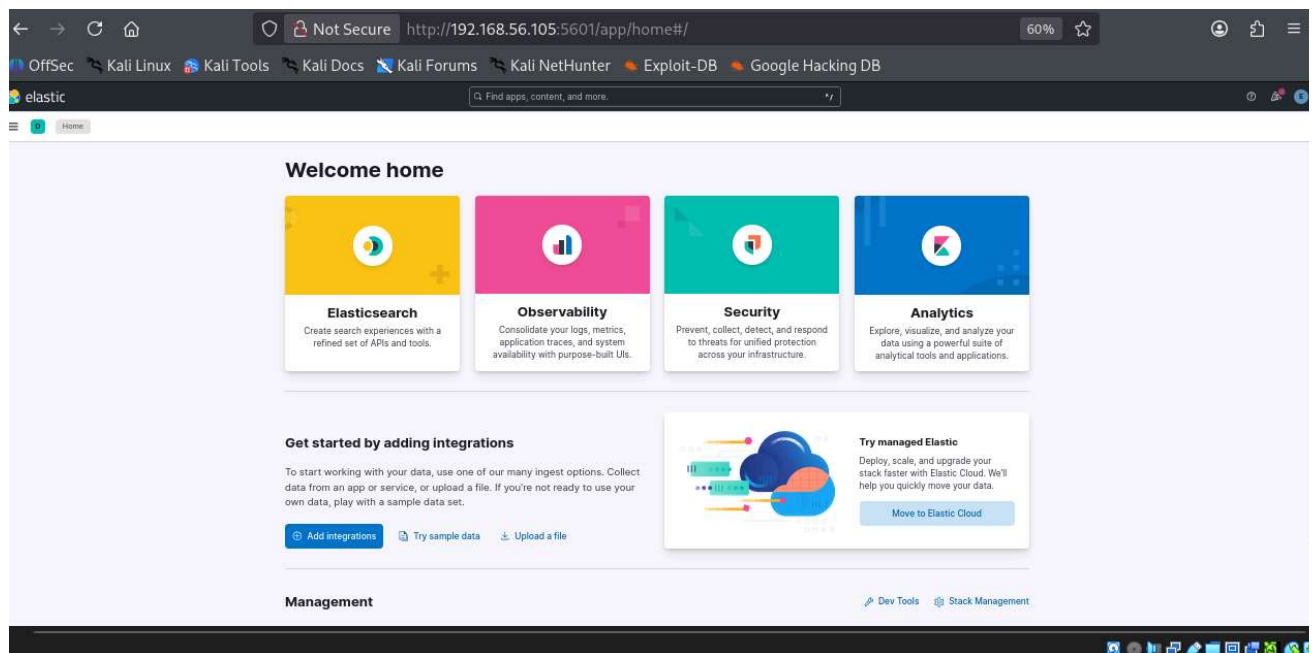


FIG.1 IMAGE INDICATING SIEM DASHBOARD ON ELK

Create data view

Name

filebeat

Index pattern

filebeat-*

Timestamp field

@timestamp

Select a timestamp field for use with the global time filter.

[Show advanced settings](#)

[Close](#) [Save data view to Kibana](#)

FIG.2 IMAGE INDICATING CREATION OF A DATA VIEW

Data views filebeat [Delete](#) [Edit](#)

Index pattern: filebeat-* Time field: @timestamp [Default](#)

[Fields \(6649\)](#) [Scripted fields \(0\)](#) [Field filters \(0\)](#) [Relationships \(0\)](#)

Field type: 36 Schema type: [Refresh](#) [Add field](#)

Name ↑	Type ↓	Format	Searchable	Aggregatable	Excluded	Actions
@timestamp	date		•	•		Edit
_id	_id		•			Edit
_ignored	_ignored		•	•		Edit
_index	_index		•	•		Edit
_score						Edit
_source	_source					Edit
activemq.caller	keyword		•	•		Edit
activemq.log_stack_trace	keyword		•	•		Edit
activemq.thread	keyword		•	•		Edit
activemq.user	keyword		•	•		Edit

Rows per page: 10 [1](#) [2](#) [3](#) [4](#) [5](#) [665](#)

FIG.3 IMAGE INDICATING SUCCESSFUL CREATION OF DATA VIEW

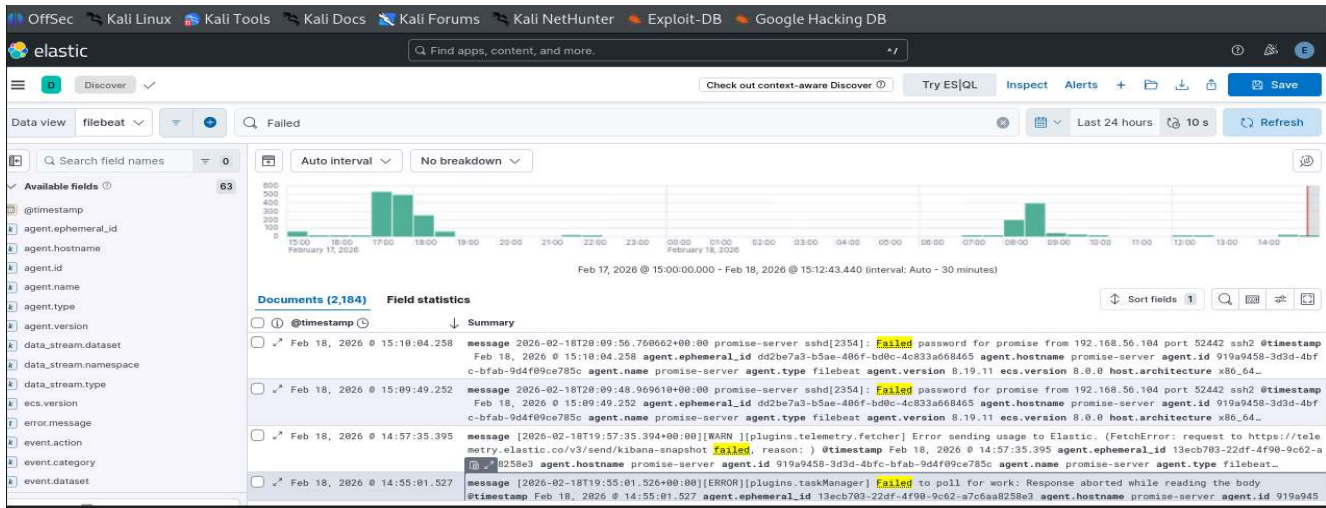


FIG. 4 IMAGE INDICATING SIEM DETECTING FAILED SSH ATTEMPTS

```
(kali@kali)-[~]
$ hydra -t 4 -l promise -P /usr/share/wordlists/rockyou.txt 192.168.56.105 ssh

Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-18 15:41:34
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.rest
ore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.105:22/
[STATUS] 68.00 tries/min, 68 tries in 00:01h, 14344331 to do in 3515:47h, 4 active
[STATUS] 70.33 tries/min, 211 tries in 00:03h, 14344188 to do in 3399:06h, 4 active
[STATUS] 68.00 tries/min, 476 tries in 00:07h, 14343923 to do in 3515:41h, 4 active
```

FIG 5 IMAGE INDICATING USE OF HYDRA FOR BRUTE FORCE ATTACK



FIG.6 IMAGE INDICATING SIEM DETECTING BRUTE FORCE ATTACK

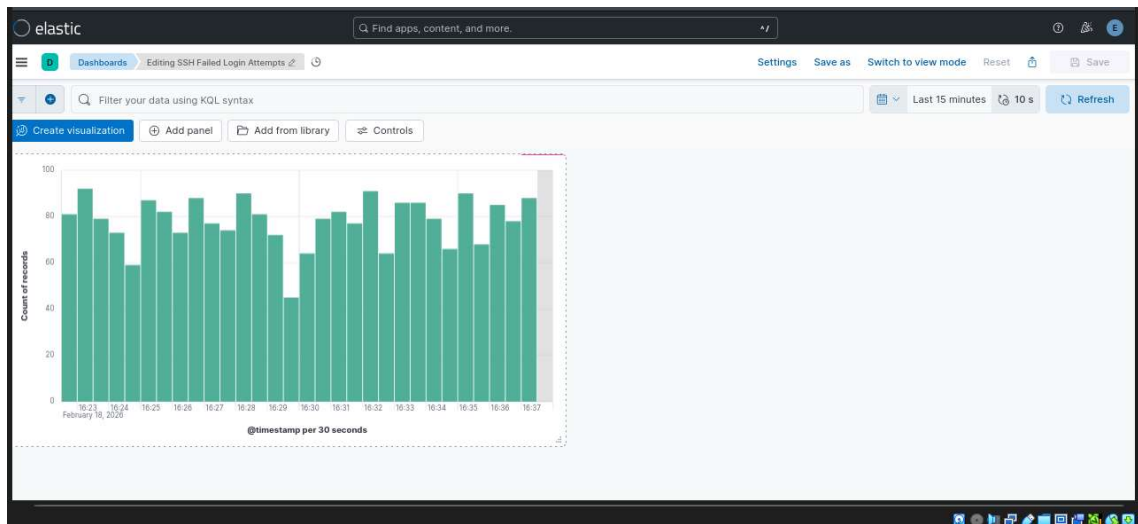


FIG 7. IMAGE INDICATING SIEM DASHBOARD