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

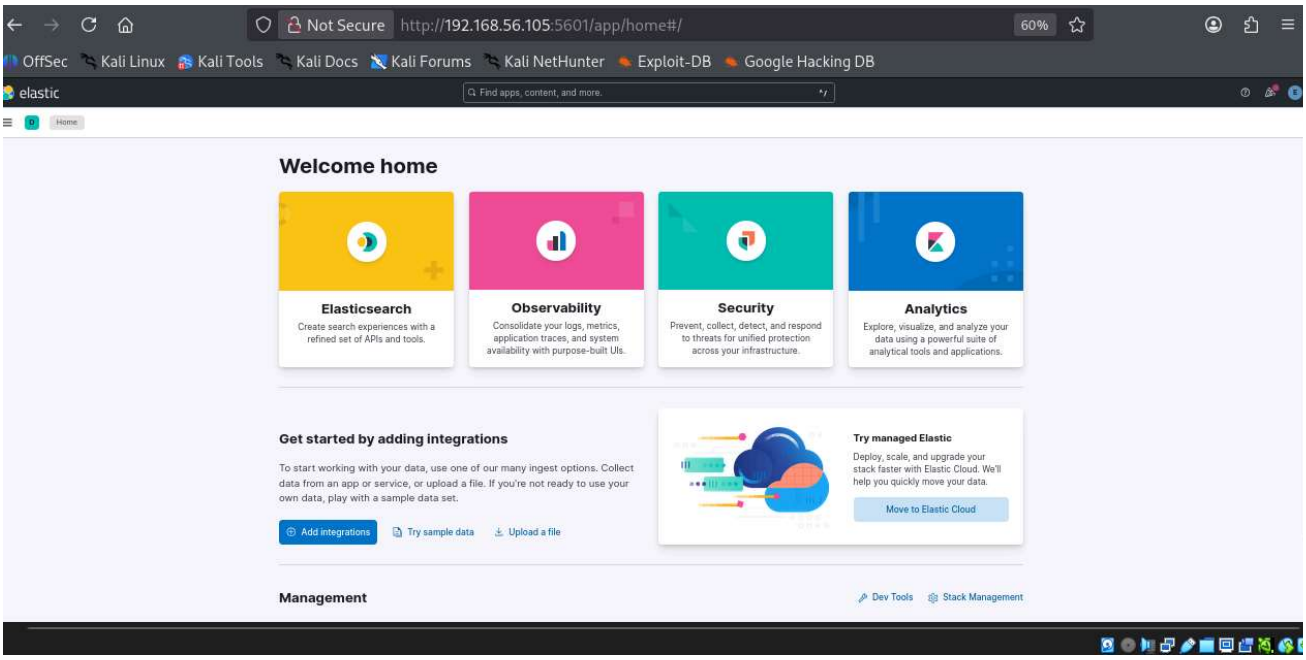

FIG.1 IMAGE INDICATING SIEM DASHBOARD ON ELK

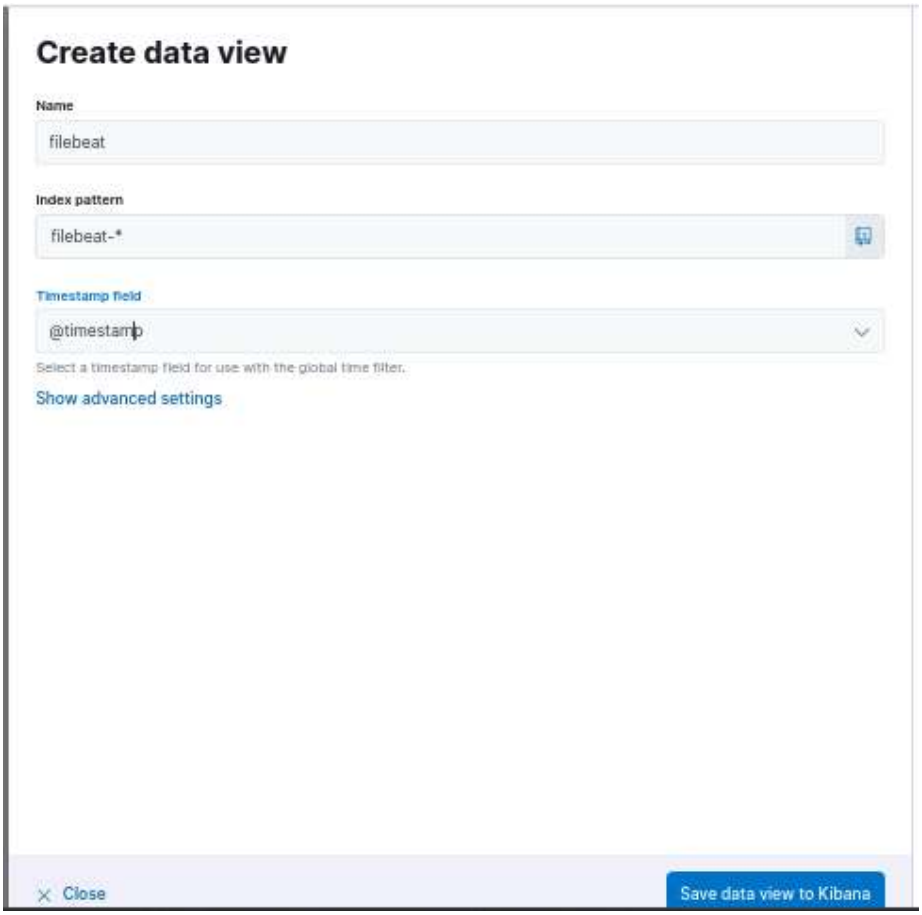

FIG.2 IMAGE INDICATING CREATION OF A DATA VIEW

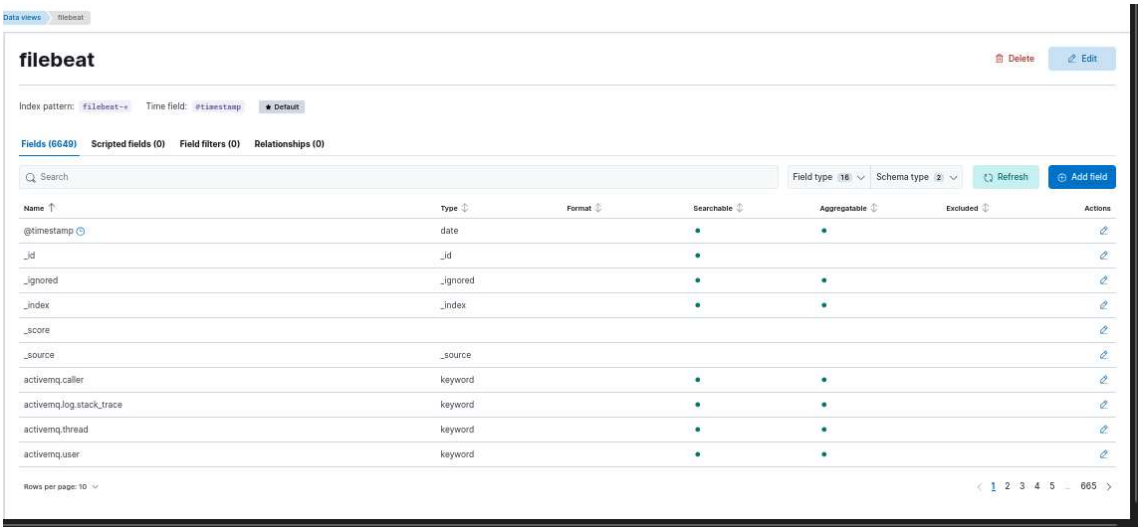

FIG.3 IMAGE INDICATING SUCCESSFUL CREATION OF DATA VIEW

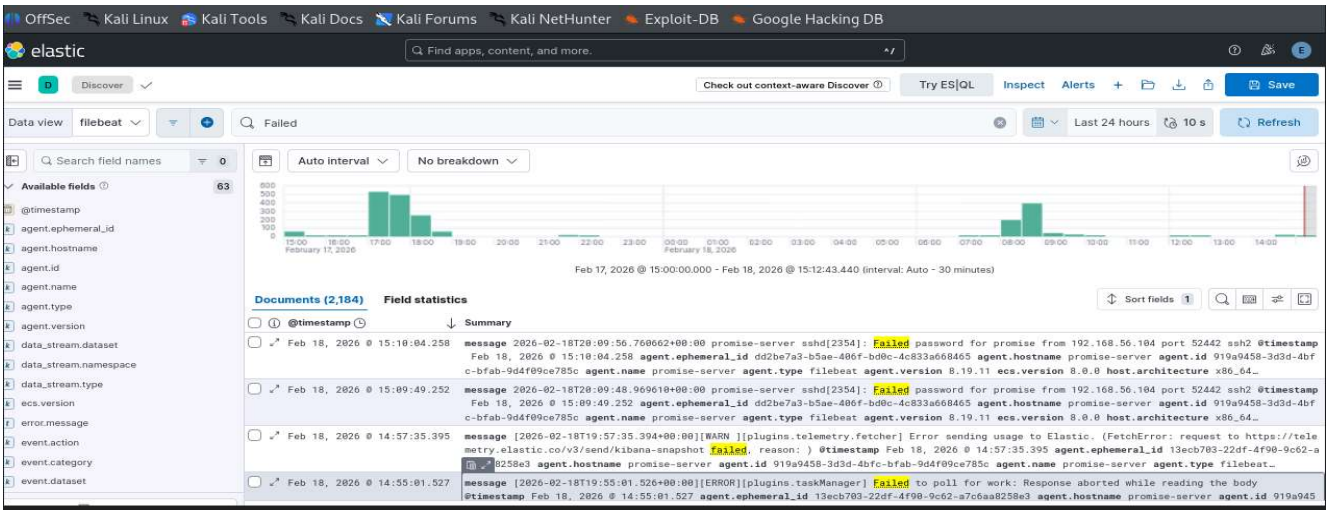

FIG. 4 IMAGE INDICATING SIEM DETECTING FAILED SSH ATTEMPTS

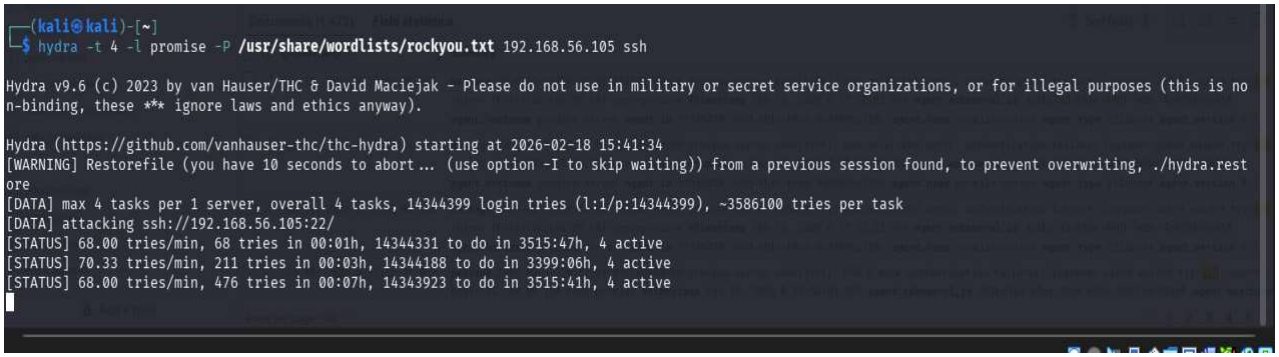

FIG 5 IMAGE INDICATING USE OF HYDRA FOR BRUTE FORCE ATTACK

FIG .6 IMAGE INDICATING SIEM DETECTING BRUTE FORCE ATTACK

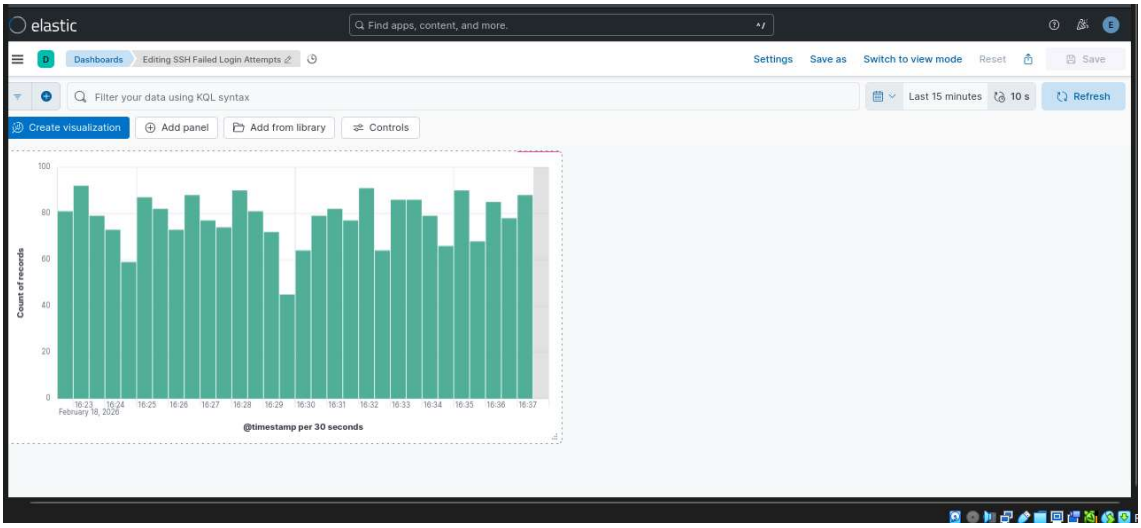

FIG 7. IMAGE INDICATING SIEM DASHBOARD