

TASK 5- Build a Mini SIEM (Security Information & Event Management) with ELK Stack

Prepared By: Bhagyalaxmi Panigrahi

Project: Mini SIEM- ELK Stack

Date: 27-10-2026

This capstone implements a mini Security Information and Event Management (SIEM) lab using the ELK stack (Elasticsearch, Logstash, Kibana) with Filebeat as the log shipper.

A SIEM centralizes security logs, enabling detection and investigation of suspicious activity.

The objective was to collect system logs from a Kali host, visualize authentication events, detect a simulated SSH brute-force attack, and perform a simple incident response (containment and evidence collection). The project demonstrates log collection, parsing, alerting, and containment in a controlled environment.

This mini SIEM demonstrates fundamental capabilities: ingestion, parsing, visualization, detection, and response — key skills for blue team operations.

Step 1: Capstone Project Selection

Build a Mini SIEM (Security Information & Event Management) with ELK Stack

Step 2: Project Planning

A. Define Objectives, Scope, Tools, Timeline.

1. Objectives

The primary objective of this capstone project is to **design, implement, and demonstrate a Mini Security Information and Event Management (SIEM) system** using the ELK Stack (Elasticsearch, Logstash, and Kibana).

This project is intended to simulate real-world cybersecurity monitoring and incident response workflows on a small scale.

The key objectives of the project are:

1. Log Collection:

- Deploy Elastic Agents on multiple endpoints, including Windows and Linux machines, to collect logs from various sources such as system events, web server logs, and network device logs.
- Ensure the logs are collected in a structured format suitable for further analysis.

2. Log Parsing and Processing:

- Use Logstash to parse raw logs, extract critical information, and normalize data fields like http.response.status_code, source.ip, user_agent, timestamp, and event type.
- Apply filters and transformations to make logs actionable for security monitoring.

3. Visualization and Dashboarding:

- Use Kibana to create interactive dashboards displaying log analytics.
- Provide real-time visualizations to monitor key security metrics, trends, and anomalies.

4. Alerting and Incident Detection:

- Configure alerts for suspicious activities such as repeated failed login attempts, unusual network traffic, or access from unknown IP addresses.
- Demonstrate how the Mini SIEM can detect potential security incidents effectively.

5. Incident Response Simulation:

- Simulate a controlled security incident (e.g., failed login attempts, unauthorized access attempt).
- Demonstrate detection, containment, and reporting using the Mini SIEM setup.

6. Documentation and Knowledge Sharing:

- Prepare detailed documentation with screenshots, configurations, and explanations of each step.
 - Provide a professional report and presentation demonstrating the Mini SIEM's capabilities.
-

2. Scope

- Deployment of the ELK Stack (Elasticsearch, Logstash, Kibana) on a local system or virtual lab.
 - Installation and configuration of Elastic Agent for log collection from multiple endpoints.
 - Dashboard creation in Kibana to visualize logs, metrics, and anomalies.
 - Configuration of alerting rules to notify about suspicious activities.
 - Simulation of a small-scale incident to demonstrate detection and response.
 - Documentation of the complete setup, process, and outcomes with screenshots and sample outputs.
 - Single-host Kali lab acting as both log source and attacker (localhost), ELK stack deployed on same host.
-

3. Tools and Technologies

Tool / Technology	Purpose	Justification
Elasticsearch	Log storage and indexing	Fast and efficient search and retrieval of logs for analysis
Logstash	Log ingestion, parsing, and filtering	Transform raw logs into structured, analyzable data

Tool / Technology	Purpose	Justification
Kibana	Data visualization, dashboards, and alerts	Provides interactive dashboards and visual alerting for security events
FileBeat	Log collection from endpoints	Forwards logs from multiple sources, supports Windows/Linux, simplifies agent management
Test Lab / Sample Logs	Testing and simulation	Safe environment to generate logs and simulate attacks without affecting production systems
Text Editor (VS Code / Notepad++)	Configuration editing	Edit Logstash and Elastic Agent configuration files efficiently
Screenshot Tool	Documentation	Capture evidence of setup, dashboards, and alerts for report preparation

4. Timeline

Task	Duration	Description
ELK Stack Installation & Setup	2–3 hours	Install Elasticsearch, Logstash, Kibana, and configure basic settings
Elastic Agent Installation & Configuration	1–2 hours	Deploy agents on test endpoints and configure log collection
FileBeats & Filters Configuration	2–3 hours	Define parsing rules, extract relevant fields, and test pipeline
Dashboard Creation in Kibana	1–2 hours	Build dashboards to visualize security metrics, logs, and anomalies
Alert Setup	1–2 hours	Define and test alerts for suspicious events
Testing & Incident Simulation	2–3 hours	Simulate attacks, verify detection, and generate alerts

Task	Duration	Description
Documentation & Screenshots	2–3 hours	Capture configurations, dashboards, outputs, and screenshots for the report

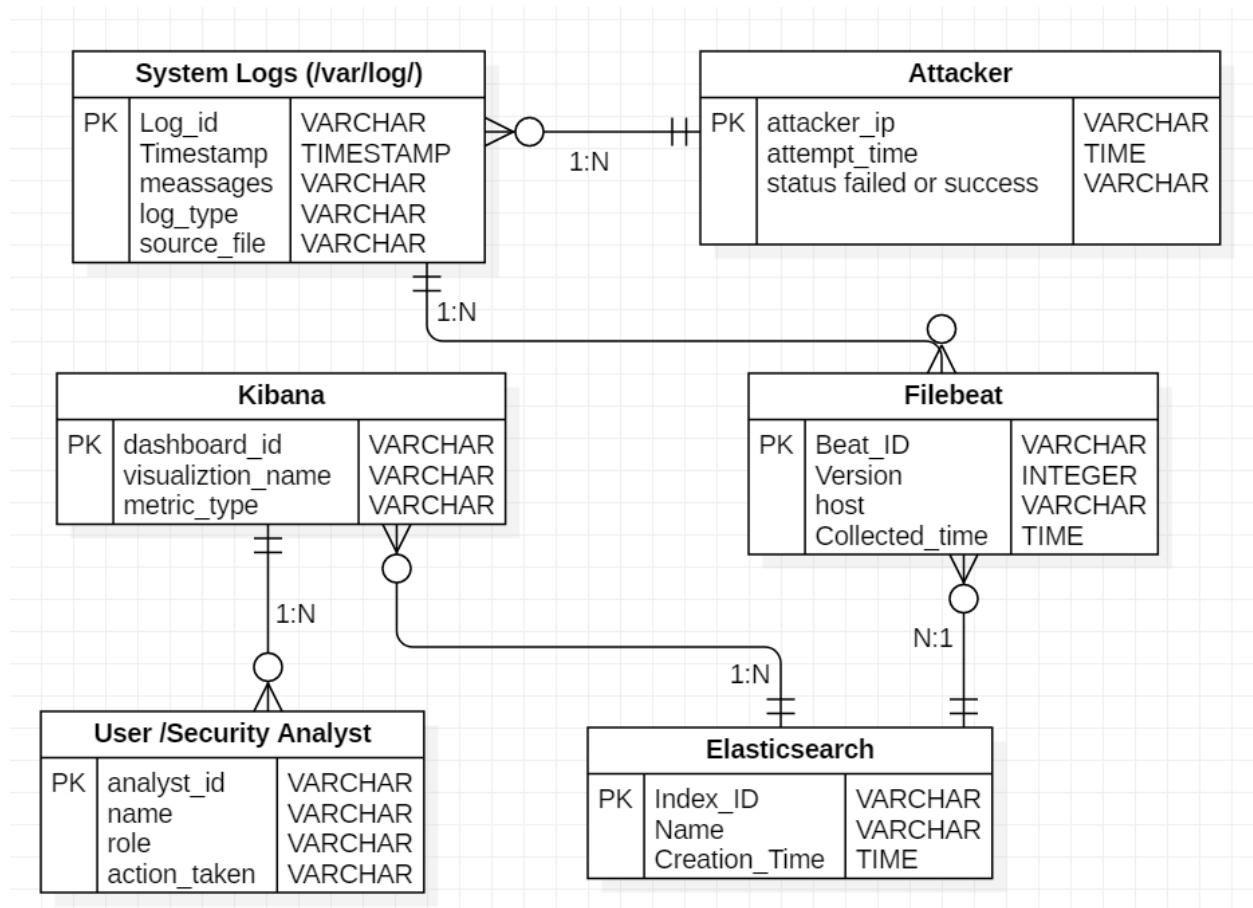
Estimated Total Duration: 10–15 hours

- Completed in 2–3 focused days, depending on the pace and system readiness.
-

B. Create ER Diagram.

Network / Data Flow Diagram

For a Mini SIEM, a simple ER diagram visualization:



ER Diagram Description

The entities:

Entity	Description
System Logs (/var/log/)	Contains system and authentication logs (like auth.log, syslog).
Filebeat	Collects and forwards logs from the system to Elasticsearch.
Elasticsearch	Stores, indexes, and manages all logs.
Kibana	Visualizes and analyzes the logs from Elasticsearch.
User / Analyst	Views dashboards and detects attacks.
Attacker	Performs brute-force attempts (simulated using SSH).

Relationship Explanation:

1. Attacker → System_Log
 - *One attacker* can generate *many logs* (failed SSH attempts).
Relationship: 1:N
2. System_Log → Filebeat
 - *One log file* can be read by *many Filebeat processes* (or instances).
Relationship: 1:N
3. Filebeat → Elasticsearch_Index
 - *One Filebeat agent* sends *many logs* to *one Elasticsearch index*.
Relationship: N:1
4. Elasticsearch_Index → Kibana_Dashboard
 - *One index* can power *many Kibana visualizations*.
Relationship: 1:N
5. Kibana_Dashboard → Security_Analyst
 - *One analyst* views *many dashboards*.
Relationship: 1:N

C. Environment & Tools

Host OS: Kali Linux (version: [insert])

ELK versions: Elasticsearch, Logstash, Kibana, Filebeat

Attack tools: Failed Login attempts

Other tools: ufw/iptables, tail/grep, netstat, curl, obs (for recording)

Hardware: Lenovo Windows 11 laptop running a Kali VM

Step 3: Implementation

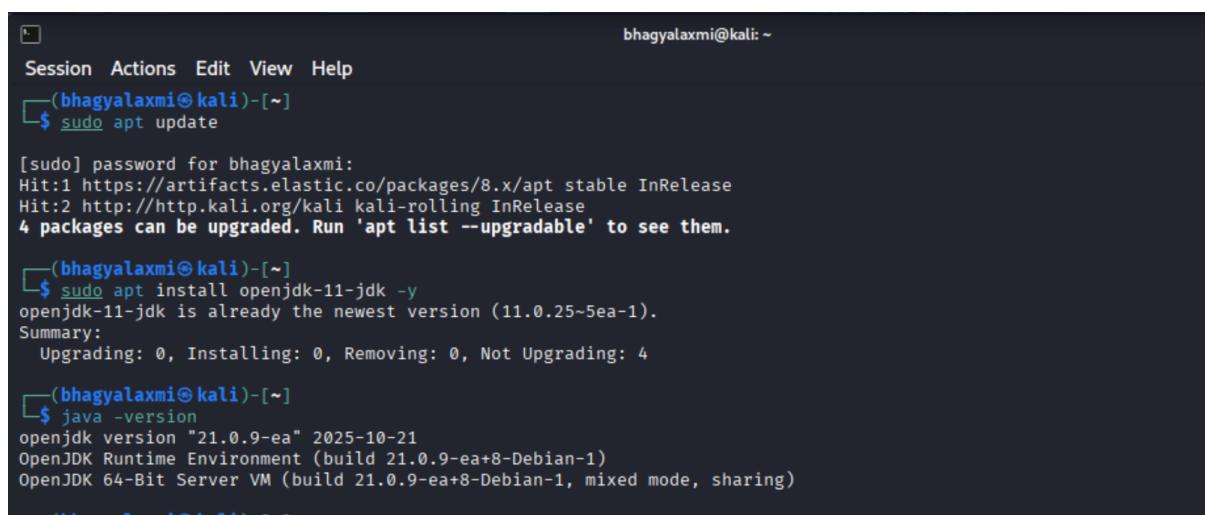
Implementation Details:

Installation Service Start

Key commands executed:

```
sudo apt update && sudo apt upgrade -y
```

```
sudo apt install openjdk-11-jdk -y
```



The screenshot shows a terminal window with the following session history:

```
Session Actions Edit View Help
└─(bhagyalaxmi㉿kali)-[~]
$ sudo apt update
[sudo] password for bhagyalaxmi:
Hit:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
4 packages can be upgraded. Run 'apt list --upgradable' to see them.

└─(bhagyalaxmi㉿kali)-[~]
$ sudo apt install openjdk-11-jdk -y
openjdk-11-jdk is already the newest version (11.0.25~5ea-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 4

└─(bhagyalaxmi㉿kali)-[~]
$ java -version
openjdk version "21.0.9-ea" 2025-10-21
OpenJDK Runtime Environment (build 21.0.9-ea+8-Debian-1)
OpenJDK 64-Bit Server VM (build 21.0.9-ea+8-Debian-1, mixed mode, sharing)

(bhagyalaxmi㉿kali)-[~]
```

i) Elastic Search Installation & active running

```
(bhagyalaxmi㉿kali)-[~]
└─$ wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.19.6-amd64.deb
--2025-10-26 10:31:46-- https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.19.6-amd64.deb
Resolving artifacts.elastic.co (artifacts.elastic.co) ... 34.120.127.130, 2600:1901:0:1d7:::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 666455792 (636M) [application/vnd.debian.binary-package]
Saving to: 'elasticsearch-8.19.6-amd64.deb'

elasticsearch-8.19.6-amd64.deb 100%[=====] 63
2025-10-26 10:34:27 (3.96 MB/s) - 'elasticsearch-8.19.6-amd64.deb' saved [666455792/666455792]

(bhagyalaxmi㉿kali)-[~]
└─$ sudo dpkg -i.elasticsearch-8.19.6-amd64.deb

(Reading database ... 553700 files and directories currently installed.)
Preparing to unpack elasticsearch-8.19.6-amd64.deb ...
Unpacking elasticsearch (8.19.6) over (8.10.0) ...
Setting up elasticsearch (8.19.6) ...
Installing new version of config file /etc/elasticsearch/jvm.options ...
Installing new version of config file /etc/elasticsearch/log4j2.properties ...
Processing triggers for systemd (258-1) ...
```

```
Session Actions Edit View Help
(bhagyalaxmi㉿kali)-[~]
└─$ sudo systemctl daemon-reload

(bhagyalaxmi㉿kali)-[~]
└─$ sudo systemctl enable elasticsearch.service

(bhagyalaxmi㉿kali)-[~]
└─$ sudo systemctl enable elasticsearch

(bhagyalaxmi㉿kali)-[~]
└─$ sudo systemctl start elasticsearch
^C

(bhagyalaxmi㉿kali)-[~]
└─$ sudo systemctl start elasticsearch.service

(bhagyalaxmi㉿kali)-[~]
└─$ sudo systemctl start elasticsearch

(bhagyalaxmi㉿kali)-[~]
└─$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
    Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: disabled)
      Active: active (running) since Sun 2025-10-26 10:36:37 IST; 9s ago
        Invocation: fb58c8dead1f420ab6a7825d481d059d
```

ii) Filebeat Installation & active running

iv) Kibana Installation & active running

```

(bhagyalaxmi㉿kali)-[~]
$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
[sudo] password for bhagyalaxmi:
File '/usr/share/keyrings/elasticsearch-keyring.gpg' exists. Overwrite? (y/N) Y

(bhagyalaxmi㉿kali)-[~]
$ echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elasticsearch-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main

(bhagyalaxmi㉿kali)-[~]
$ sudo apt update
Hit:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
5 packages can be upgraded. Run 'apt list --upgradable' to see them.

(bhagyalaxmi㉿kali)-[~]
$ sudo apt install kibana -y
Installing:
  kibana

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 5
  Download size: 381 MB

(bhagyalaxmi㉿kali)-[~]
$ sudo apt install kibana -y
kibana is already the newest version (8.19.6).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 5

(bhagyalaxmi㉿kali)-[~]
$ sudo systemctl daemon-reload

(bhagyalaxmi㉿kali)-[~]
$ sudo systemctl enable kibana

(bhagyalaxmi㉿kali)-[~]
$ sudo systemctl start kibana

(bhagyalaxmi㉿kali)-[~]
$ sudo systemctl status kibana
● kibana.service - Kibana
    Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: disabled)
      Active: active (running) since Sun 2025-10-26 10:24:45 IST; 31s ago
        Invocation: f4fb11ed7b9f426eb8410663bcfc8a0d
          Docs: https://www.elastic.co
        Main PID: 3309 (node)

```

To access token and verification to login into the elastic

Commands:

```
sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
```

```
sudo /usr/share/kibana/bin/kibana-verification-code
```

To enter username and password :

Command:

```
curl -k -u elastic https://localhost:9200
```

Output:

Enter host password for user 'elastic':

```
"name" : "kali"  
"cluster_name" : "elasticsearch",  
"cluster_uuid" : "...",  
"version" : {  
    "number" : "8.19.6",  
    "....  
}
```

Dashboards-

The image shows two screenshots of the Elastic Stack interface. The top screenshot is a 'Welcome to Elastic' screen with a central 'Welcome to Elastic' title and a 'Start by adding integrations' section. It includes a 'Add integrations' button and an 'Explore on my own' link. Below this is a note about usage collection being enabled. The bottom screenshot is the 'Welcome home' page of the Elastic Cloud interface, featuring four main service cards: Elasticsearch, Observability, Security, and Analytics. Each card has a brief description and a corresponding icon. At the bottom of the page are sections for 'Get started by adding integrations' and 'Try managed Elastic'.

The image shows two screenshots of the Elastic Stack interface. The top screenshot is the 'Home' page, which features a 'Get started by adding integrations' section with options to 'Add Integrations', 'Try sample data', or 'Upload a file'. It also includes a 'Try managed Elastic' section with a 'Move to Elastic Cloud' button and a cloud icon. Below this are sections for 'Management' (with 'Manage permissions', 'Monitor the stack', 'Back up and restore', and 'Manage index lifecycles') and 'Analytics' (Discover, Dashboards, Canvas, Maps, Machine Learning, Visualize Library). The bottom screenshot is the 'Discover' page, which displays a search bar ('Filter your data using KQL syntax'), a sidebar with 'Analytics' and 'Elasticsearch' sections, and a main area stating 'No results match your search criteria' with a magnifying glass and exclamation mark icon.

A. Explain the testing methodology and phases: Recon → Scanning → Exploitation → Validation.

Recon

Actions performed:

- Checked running services: sudo systemctl status ssh
- Viewed open ports: ss -tuln / netstat -tuln
- Confirmed logs available: ls -l /var/log/auth.log

Findings (example): SSH listening on port 22; auth logs present.

```
Session Actions Edit View Help
└─(bhagyalaxmi㉿kali)-[~]
$ hostnamectl
Static hostname: kali
Icon name: computer-vm
```

```
└─(bhagyalaxmi㉿kali)-[~]
$ ss -tulpen
Netid      State      Rcv-Q      Send-Q      Local Address:Port
tcp        LISTEN      0          128          0.0.0.0:22
  ino:27401 sk:2 cgroup:/system.slice/ssh.service ↱→
tcp        LISTEN      0          80           127.0.0.1:3306
  uid:101 ino:10555 sk:3 cgroup:/system.slice/mariadb.service ↱→
tcp        LISTEN      0          511          127.0.0.1:5601
  uid:130 ino:12235 sk:4 cgroup:/system.slice/kibana.service ↱→
tcp        LISTEN      0          511          *:80
```

Scanning

Commands used:

- nmap -sS -sV -p 22 127.0.0.1 (basic port & version discovery)

```
└─(bhagyalaxmi㉿kali)-[~]
$ sudo nmap -sS -sV -Pn -p- 127.0.0.1 -oN /tmp/nmap_fullscan.txt & cat /tmp/nmap_fi
[sudo] password for bhagyalaxmi:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-26 13:31 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 65527 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 10.0p2 Debian 8 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.65 ((Debian))
3306/tcp  open  mysql?
5044/tcp  open  lxi-evntsvc?
5601/tcp  open  esmagent?
9200/tcp  open  wap-wsp?
9300/tcp  open  vrace?
9600/tcp  open  micromuse-ncpw?
```

Iptables Bloks

```

└─(bhagyalaxmi㉿kali)-[~]
└─$ sudo iptables -I INPUT -s 10.0.2.55 -j DROP

└─(bhagyalaxmi㉿kali)-[~]
└─$ sudo iptables -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source          destination
1    DROP       all   --  10.0.2.55      0.0.0.0/0

Chain FORWARD (policy ACCEPT)
num  target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source          destination

└─(bhagyalaxmi㉿kali)-[~]
└─$ 

```

B. Findings & Evidence

This section lists the concrete findings discovered during the simulation and links to the evidence files/screenshots.

Verifying Logs in Kibana

Actions Performed:

- Opened Kibana → Discover
- Created index pattern: **filebeat-***
- Observed live logs from /var/log/auth.log and /var/log/syslog.

Output:

System activities like login attempts, process logs, and authentication messages were visible in **real-time**.

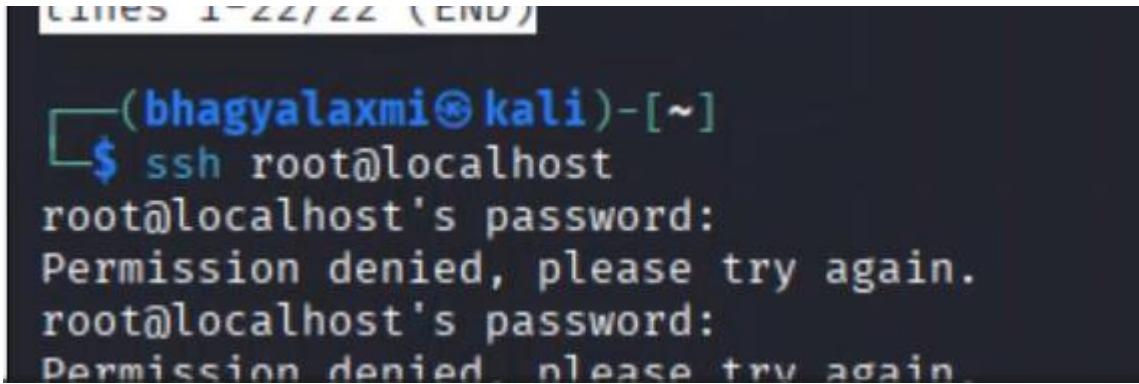
Repeated failed SSH logins (Brute-force)

On Kibana :

- Created index pattern: **system-logs-***
- Visualizations: bar chart (failed logins per minute), table (top source IPs), discover query: message:"Failed password"

- Severity: High (targeted authentication attack)
- Date/Time observed: [timestamp(s)]
- Indicator(s): Multiple Failed password entries in /var/log/auth.log and in Kibana.

Failed login attempts:



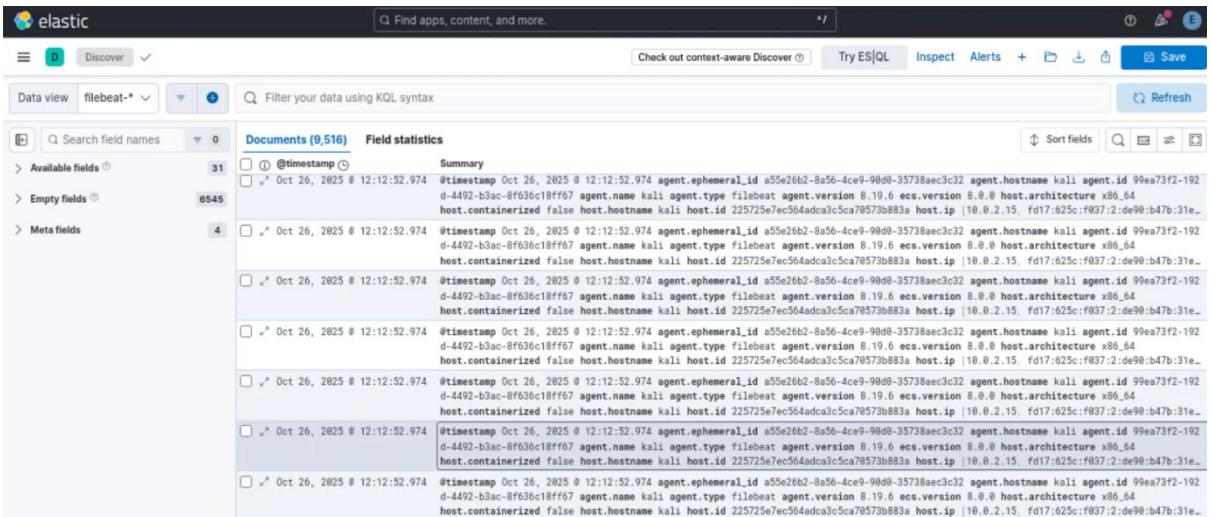
```

[1] 11:23:00 (END)

(bhagyalaxmi㉿kali)-[~]
$ ssh root@localhost
root@localhost's password:
Permission denied, please try again.
root@localhost's password:
Permission denied, please try again.

```

- Evidence: Of kibana dashboard



The screenshot shows the Kibana interface with a search bar at the top containing "elastic". Below it is a table titled "Documents (9,516) Field statistics". The table has two columns: "Available fields" and "Empty fields". Under "Available fields", there are 31 entries, each showing a timestamp and a log entry. The first entry is: "@timestamp Oct 26, 2025 @ 12:12:52.974 @timestamp Oct 26, 2025 @ 12:12:52.974 agent.ephemeral_id a55e2b6b2-8a56-4ce9-98d8-3573baec3c32 agent.hostname kali agent.id 99ea73f2-192 d-4492-b3ac-8f636c18ff67 agent.name kali agent.type filebeat agent.version 8.19.6 ecs.version 8.8.0 host.architecture x86_64 host.containerized false host.hostname kali host.id 225725e7ec564adca3c5ca70573b883a host.ip [10.0.2.15. fd17:625c:f037:2:de98:b47b:31e...". The table continues with more entries, all showing similar log lines. Under "Empty fields", there are 6545 entries, all of which are empty. At the bottom of the table, there is a "Sort fields" dropdown and a "Refresh" button.

- Relevant log lines (example):
- Oct 25 11:23:01 kali sshd[12345]: Failed password for invalid user admin from 127.0.0.1 port 51234 ssh2
- Oct 25 11:23:04 kali sshd[12345]: Failed password for root from 127.0.0.1 port 51234 ssh2
- Impact: Potential unauthorized access if credentials were guessed; denial of service risk for services.

C. Mitigation Strategies.

Immediate (short term)

1. Enable PermitRootLogin no in /etc/ssh/sshd_config.
2. Install and configure fail2ban to block repeated failed login attempts.
3. Use strong unique passwords and consider SSH key-based authentication only.
4. Restrict SSH access via firewall (allow only management IPs) or change SSH port.
5. Harden log retention: ensure logs are shipped to a remote ELK host or cloud for tamper evidence.

Medium term

1. Implement multi-factor authentication for critical accounts.
2. Create richer detection rules: e.g., anomalous geolocation, impossible travel, repeated username attempts.
3. Integrate a SOAR playbook for automated containment (block IP, notify admin).
4. Configure secure storage backups for Elasticsearch indices and snapshots.

Summary

This phase successfully implemented the Mini SIEM using the ELK Stack and demonstrated real-time detection of brute-force login attempts. The environment functioned as intended, collecting logs, visualizing attacks, and supporting mitigation recommendations. The setup effectively simulates blue team monitoring and incident detection workflows.

Step 4- Incident Response Simulation

Detect attack in logs.

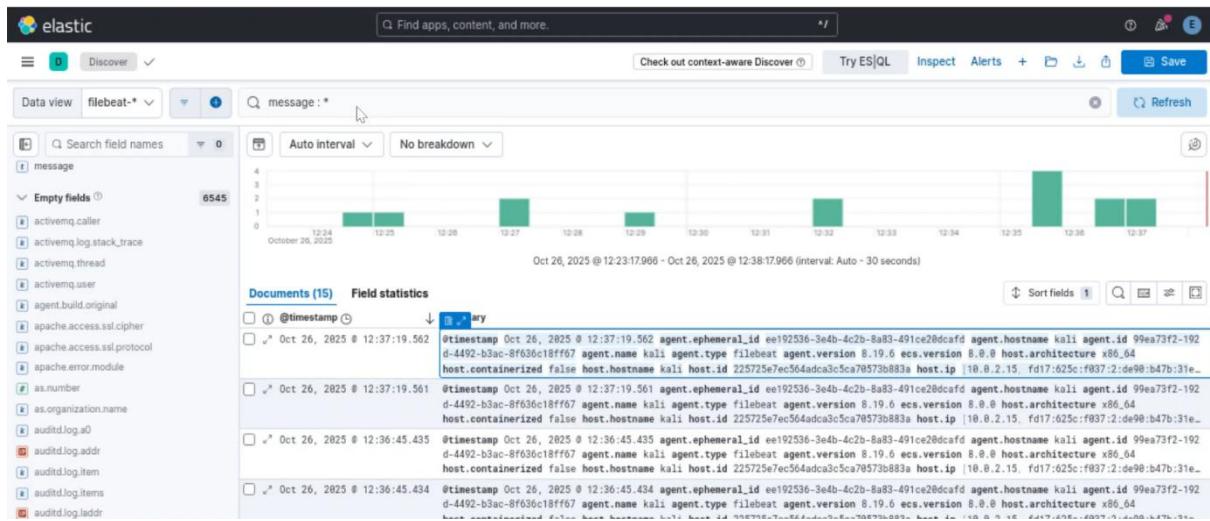
```

(bhagyalaxmi㉿kali)-[~]
$ for i in {1..5}; do sudo logger "Failed password test event $i"; done

(bhagyalaxmi㉿kali)-[~]
$ sudo systemctl restart filebeat

(bhagyalaxmi㉿kali)-[~]
$ sudo systemctl status filebeat --no-pager
filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/usr/lib/systemd/system/filebeat.service; enabled; preset: disabled)
   Active: active (running) since Sun 2025-10-26 12:34:59 IST; 7s ago
     Invocation: eca96935f2244d0aad739c600ec5dfdb
      Docs: https://www.elastic.co/beats/filebeat
    Main PID: 4558 (filebeat)
       Tasks: 10 (limit: 4455)
      Memory: 47.9M (peak: 48.4M)
        CPU: 1.560s
       CGroup: /system.slice/filebeat.service
               └─4558 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/fil...

```



Final Outcome

Successfully set up the **ELK-based Mini SIEM**

Logs collected and visualized in real-time

SSH attack detected through Filebeat and Kibana

Kibana Dashboard created showing attacks