

# **Cyber Security Internship Report at FutureInterns**

NAME : K.KAVI PREETHY

G-MAIL : [kavipreethy03@gmail.com](mailto:kavipreethy03@gmail.com)

Task 2: SECURITY ALERT MONITORING & INCIDENT  
RESPONSE

## TABLE OF CONTENT

SI NO	CONTENT	PAGE NO
1	Introduction	2
2	Objective	2
3	Tools Used	3
4	Implementation and procedure	3
5	Screenshots	4
6	Conclusion	9

## **Task 2**

# SECURITY ALERT MONITORING & INCIDENT RESPONSE

### **1. Introduction**

In modern cybersecurity operations, Security Information and Event Management (SIEM) tools play a critical role in proactively monitoring systems for suspicious activities and potential threats. This task focused on simulating a real-world Security Operations Center (SOC) scenario using Splunk, where log data was collected from a Kali Linux machine, uploaded into Splunk for analysis, and visualized on a custom dashboard. The final goal was to identify anomalies, classify incidents, and recommend appropriate responses.

### **2. Objective**

- Monitor simulated system logs using Splunk (SIEM).
- Detect and analyze potential security alerts.
- Classify detected incidents based on severity.
- Draft an incident response plan with recommendations.

### **3. Tools Used**

- OS: Kali Linux
- SIEM Tool: Splunk (Free Trial Version)
- Log Files: /var/log/ system logs (e.g., auth.log, cron, sudo logs)
- Dashboard Studio (Splunk) for visualizations

### **4.Implementation & Procedure**

#### **Step 1: Setup and Environment Preparation**

Verified presence of logs using `ls /var/log`. Selected /var/log/auth.log and similar system-generated logs that contain authentication attempts, cron jobs, and sudo usage.

#### **Step 2: Splunk Installation & Configuration**

Installed Splunk on Kali using .tgz package. Started the Splunk service:

```
sudo ./splunk start --accept-license
```

Logged into Splunk via <http://localhost:8000>

#### **Step 3: Uploading and Indexing Logs**

Navigated to 'Add Data' in Splunk, uploaded log files, selected source type (`linux\_secure`), reviewed and confirmed settings.

#### **Step 4: Log Analysis via Search**

Used Splunk Search & Reporting app, ran queries to detect patterns in sudo, and root login events.

## Step 5: Response & Recommendations

Suggested enabling alerts, limiting sudoers permissions, and regular auditing of CRON/root jobs.

## 5.Screenshort

A terminal window titled 'kali@kali: /opt/splunkbin' showing the output of the Splunk installation script. The script checks prerequisites (http, https, appserver, kvstore ports and configuration), validates indexes, and starts the Splunk server daemon. It concludes with the Splunk web interface URL at http://kali:8000.

```
kali@kali: /opt/splunkbin
File Actions Edit View Help

Checking prerequisites...
  Checking http port [8000]: open
  Checking https port [8000]: open
  Checking appserver port [127.0.0.1:8005]: open
  Checking kvstore port [8191]: open
  Checking configuration... Done
  Checking critical directories... Done
  Checking indexes...
    validated: _audit _configtracker _disappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _theishbucket histor
y main summary
  Done
  Checking filesystem compatibility... Done
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from '/opt/splunk/splunk-9.0.3-237ebbd22314-linux-amd64-manifest'
  All installed files intact.
  Done
All preliminary checks passed.

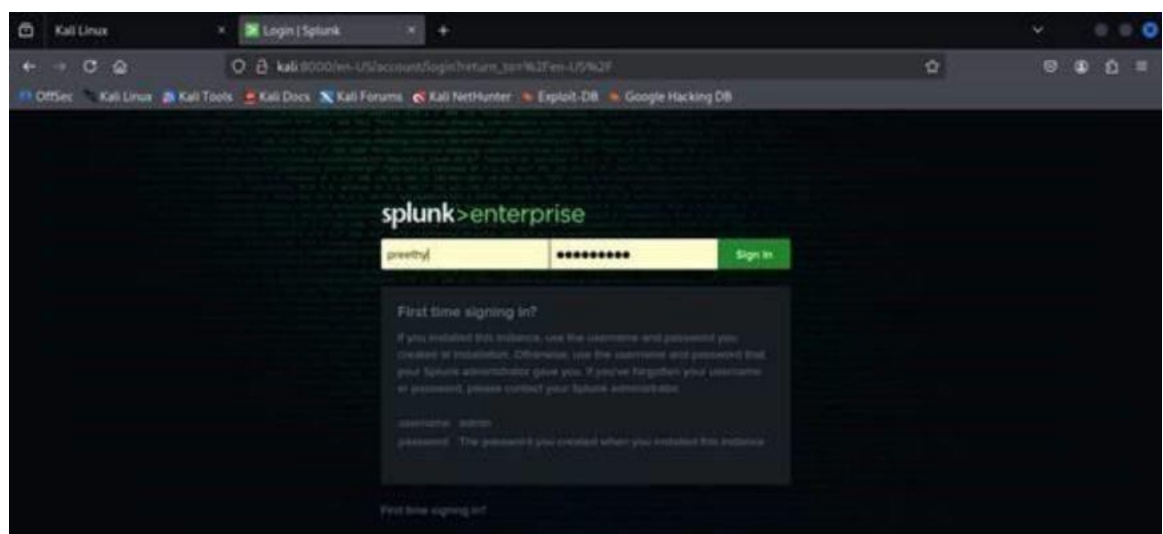
Starting splunk server daemon (splunkd)...
PRIVACY: Privacy is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

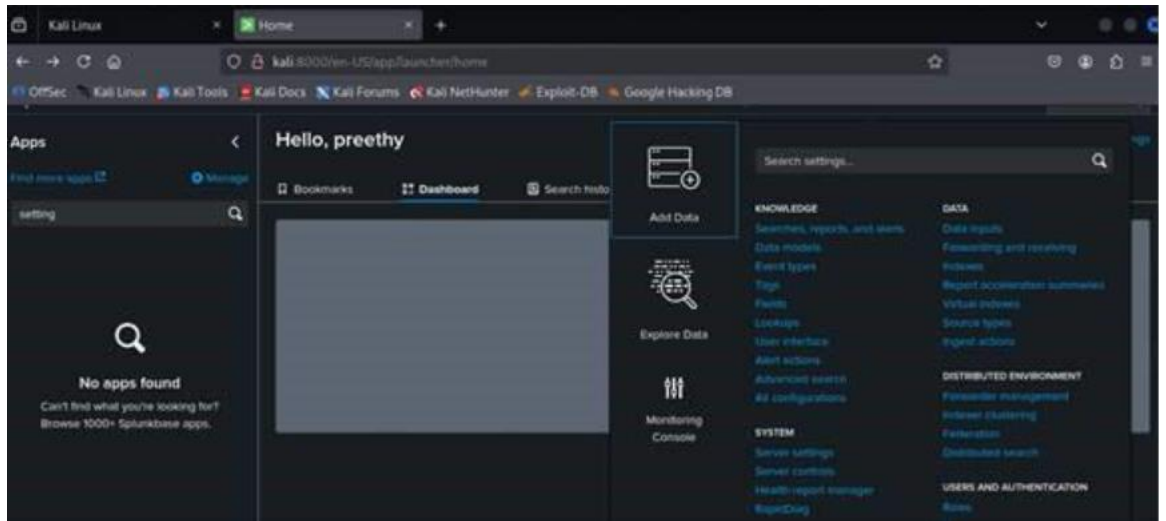
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://kali:8000
```

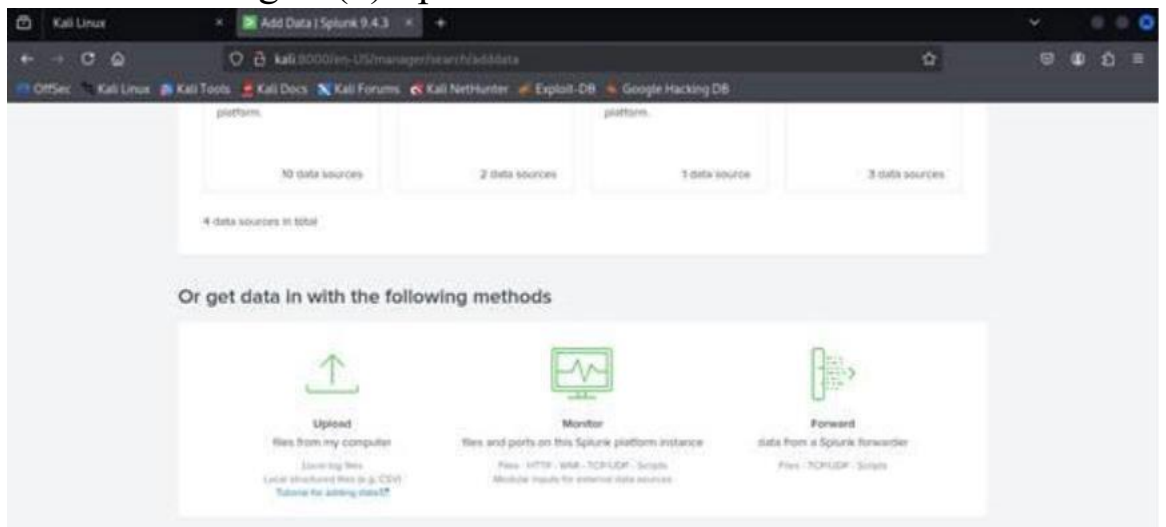
Figure(1) Started Splunk



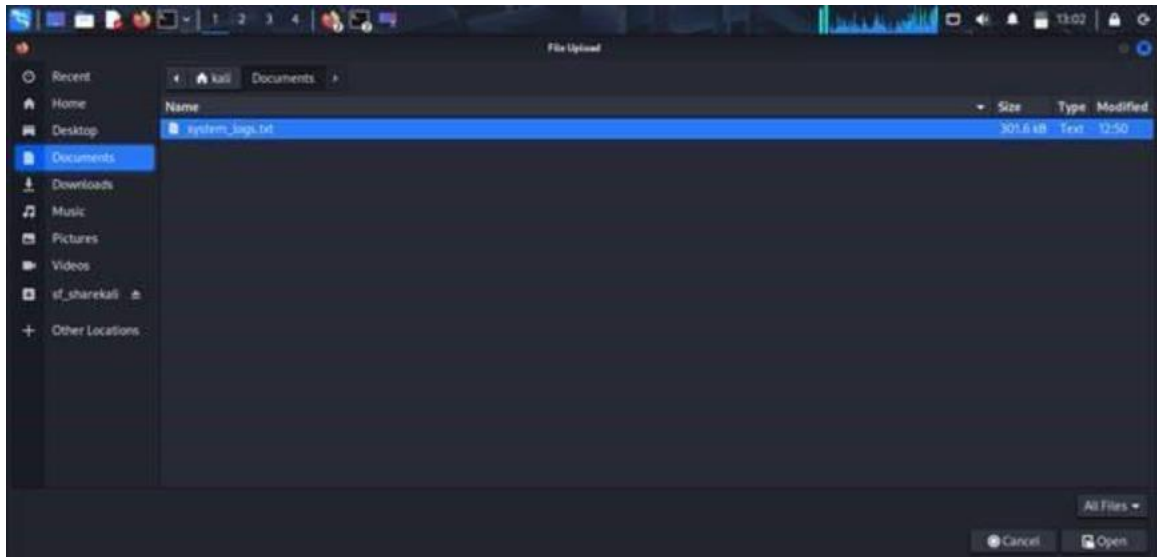
Figure(2)Login to splunk



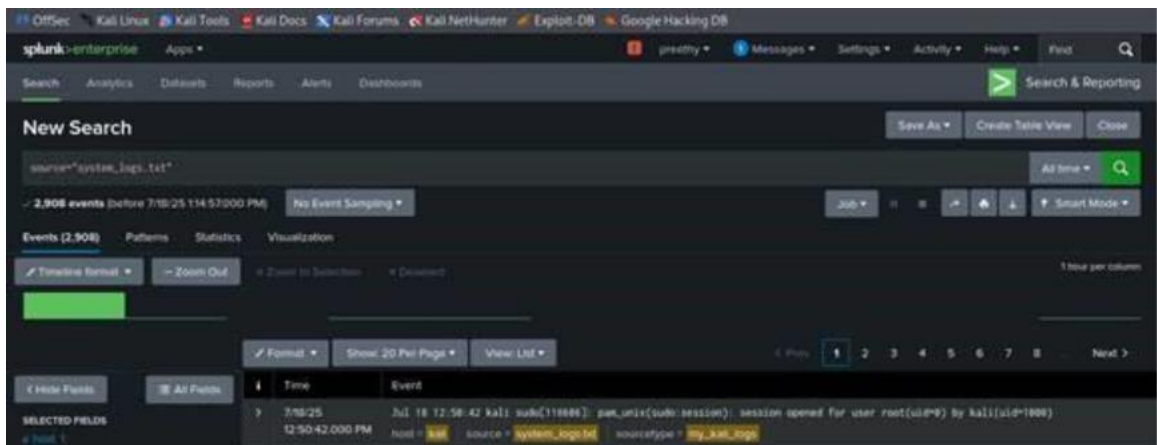
Figure(3) Splunk Dashboard



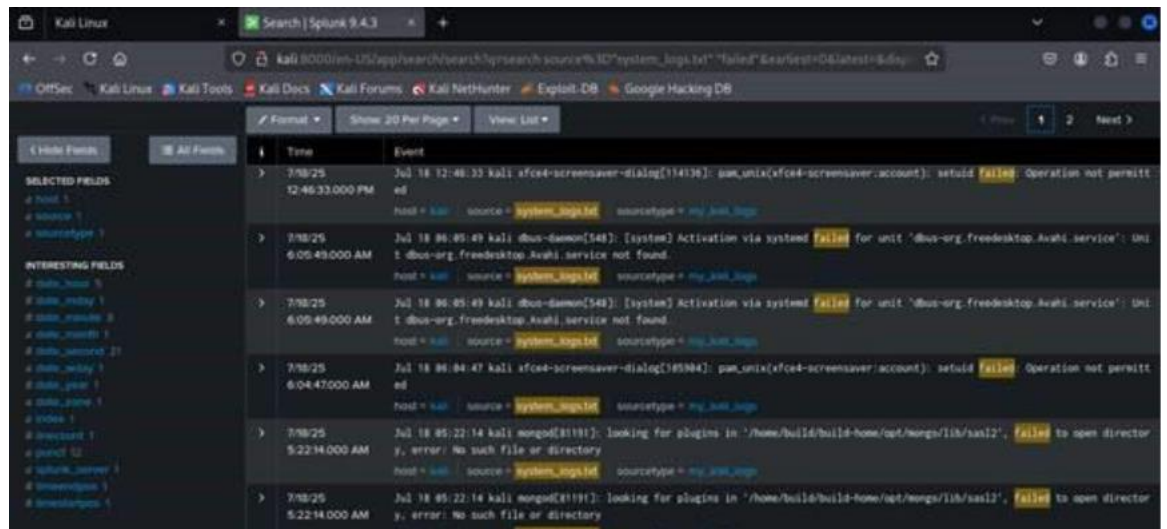
Figure(4)Uploading logs



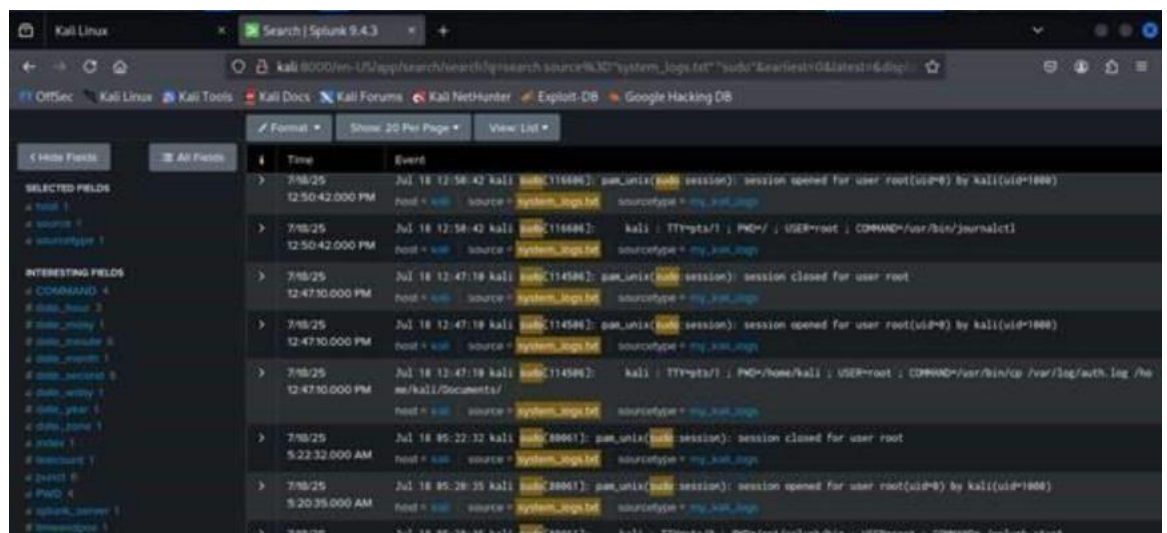
Figure(4.1) Upload the log from system



Figure(5) Analyse system\_log.text

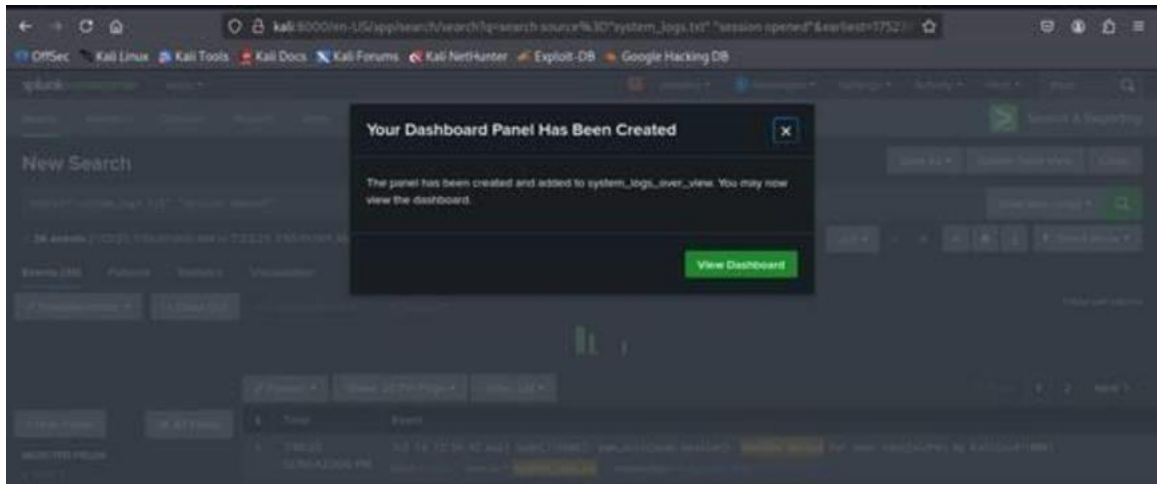


Figure(5.1)logs of failed

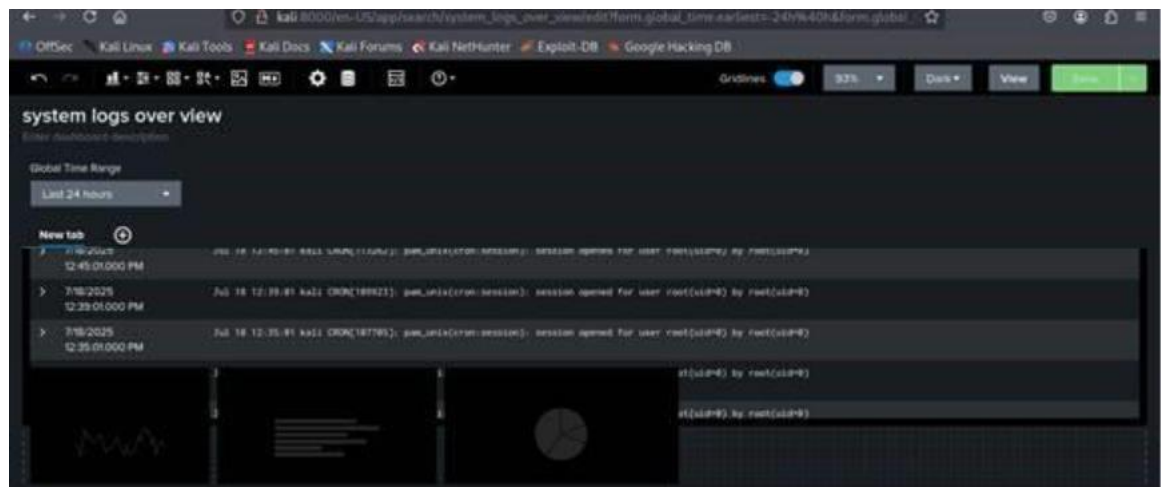


Figure(5.2).logs of sudo





Figure(5.3)Creating dashboard



Figure(5.4)graph of logs

## **6. Conclusion**

This exercise provided hands-on experience in using a SIEM tool for incident detection and response. By uploading real log files from a Kali Linux system into Splunk, the process simulated a SOC environment effectively. The visualizations enabled quick identification of suspicious activities, and the classification helped prioritize response strategies. This task enhanced my understanding of:

- Log analysis workflows
- Incident triage
- Using dashboards for real-time SOC visibility