SOC REPORT

Name: B.Pardhasaradhi Naidu

Date: 08/11/2025

S.No	TASK
1	Create a log in kali using logger and detect it

What is SIEM?

SIEM stands for **Security Information and Event Management**.

- It collects logs and events from different systems in one place.
- It analyzes those logs to detect threats and suspicious activities.
- It gives alerts and reports for security monitoring and compliance.
- Examples: **Splunk, IBM QRadar, ArcSight, Microsoft Sentinel**.

Objective

To create a custom log entry using the logger command in Kali Linux, ingest it into Splunk, and verify its detection through Splunk's Search and Reporting interface.

- Open a terminal in Kali Linux.

  Run the command: logger "This is a test log from Splunk lab".

  Verify the log is written into /var/log/syslog: tail -n 5 /var/log/syslog.

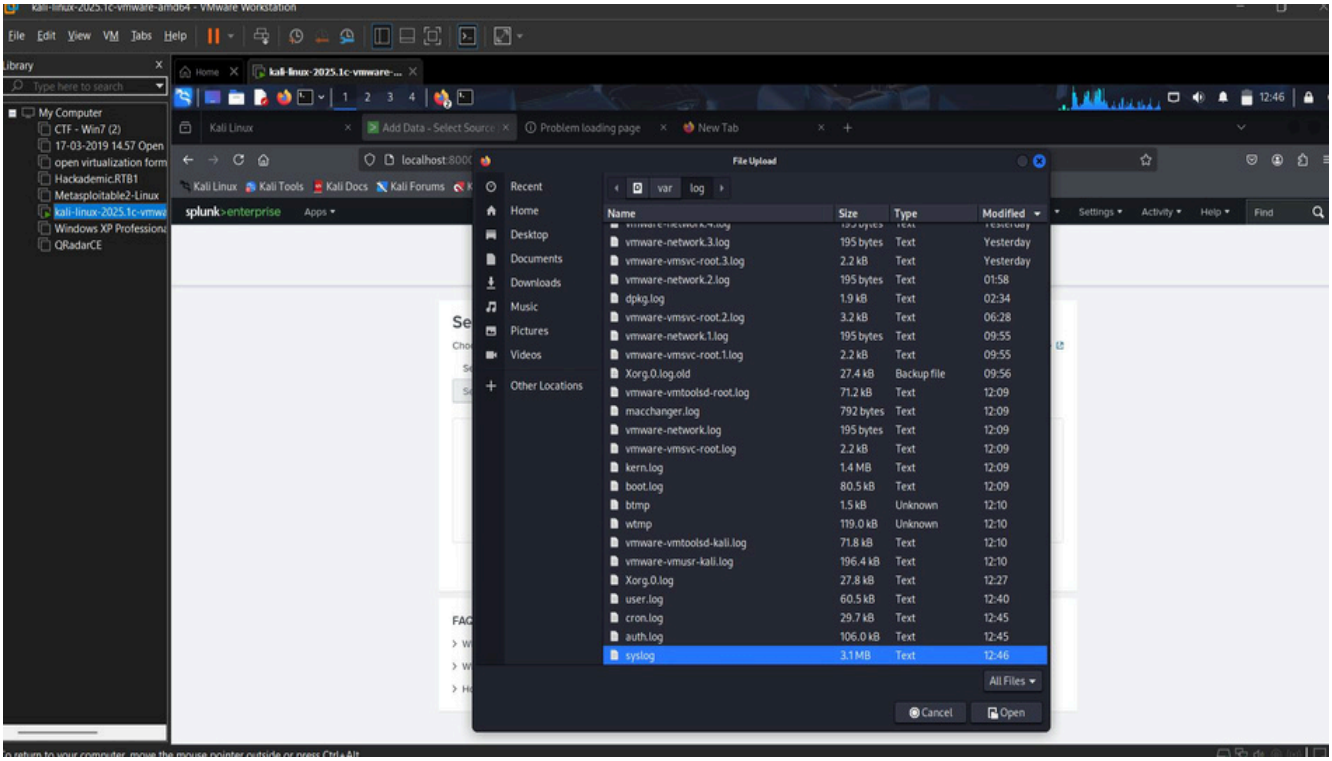
```
┌──(root㉿kali)-[/home/kali]
└─# logger "This is a test log from Splunk lab"

┌──(root㉿kali)-[/home/kali]
└─# tail -n 5 /var/log/syslog
2025-09-19T12:40:19.274121-04:00 kali systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service ...
2025-09-19T12:40:19.394781-04:00 kali dbus-daemon[587]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
2025-09-19T12:40:19.395359-04:00 kali systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher Service.
2025-09-19T12:40:22.023084-04:00 kali root: This is a test log from Splunk lab
2025-09-19T12:40:29.413767-04:00 kali systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
```

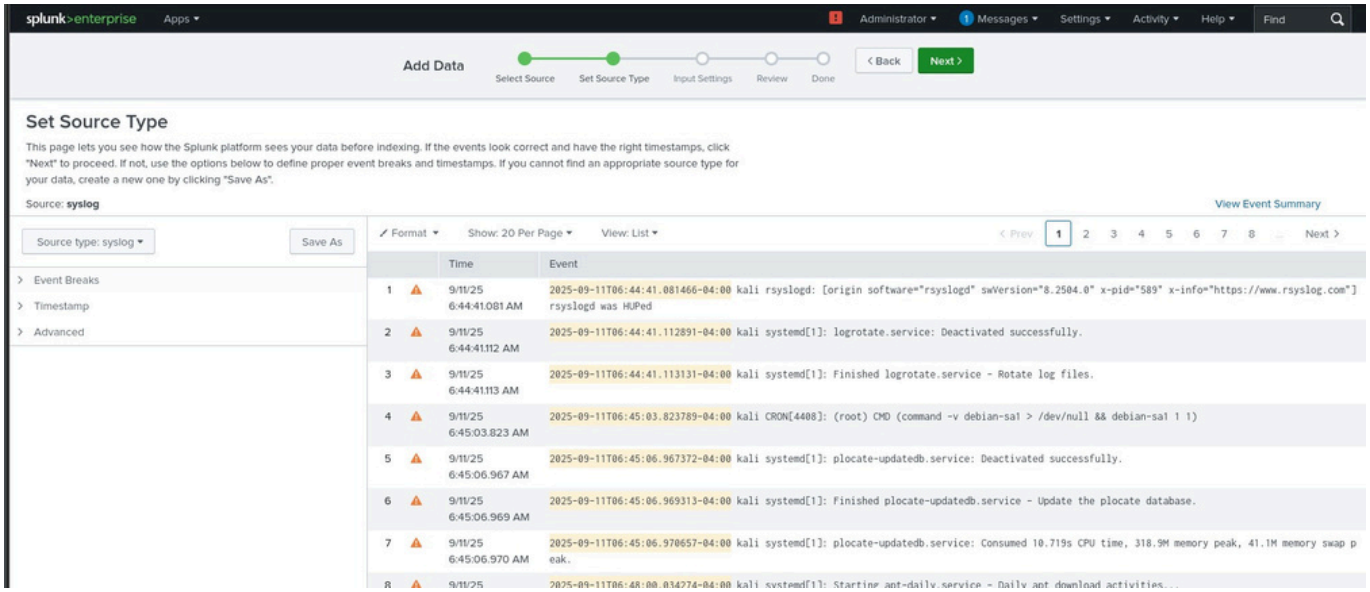
Open Splunk Web at http://localhost:8000

Navigate to: Settings → Add Data → Files & Directories.

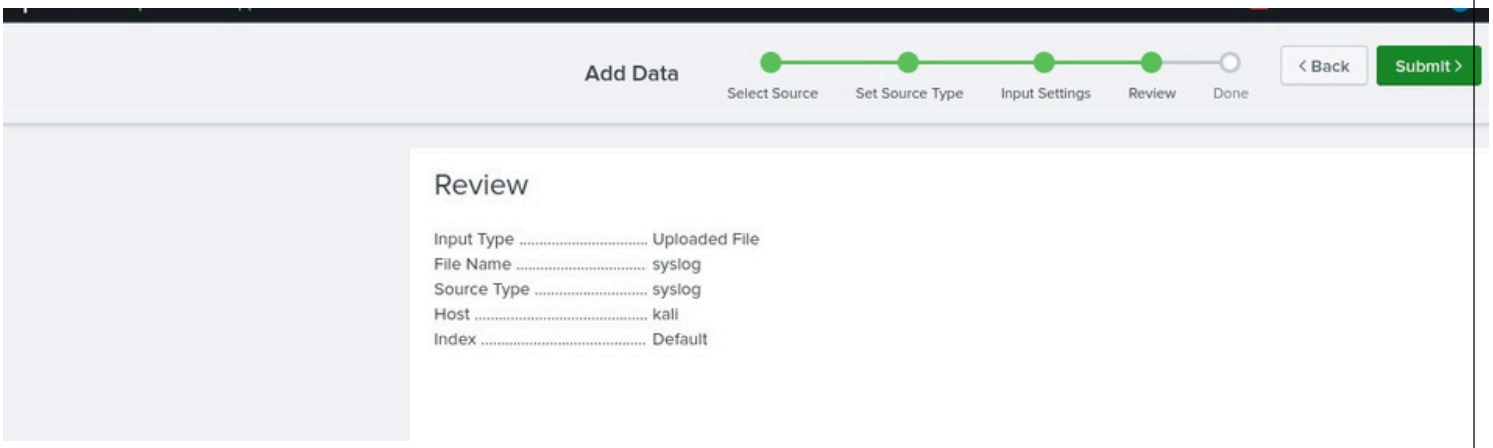
Browse and select /var/log/syslog.



Set the following options:



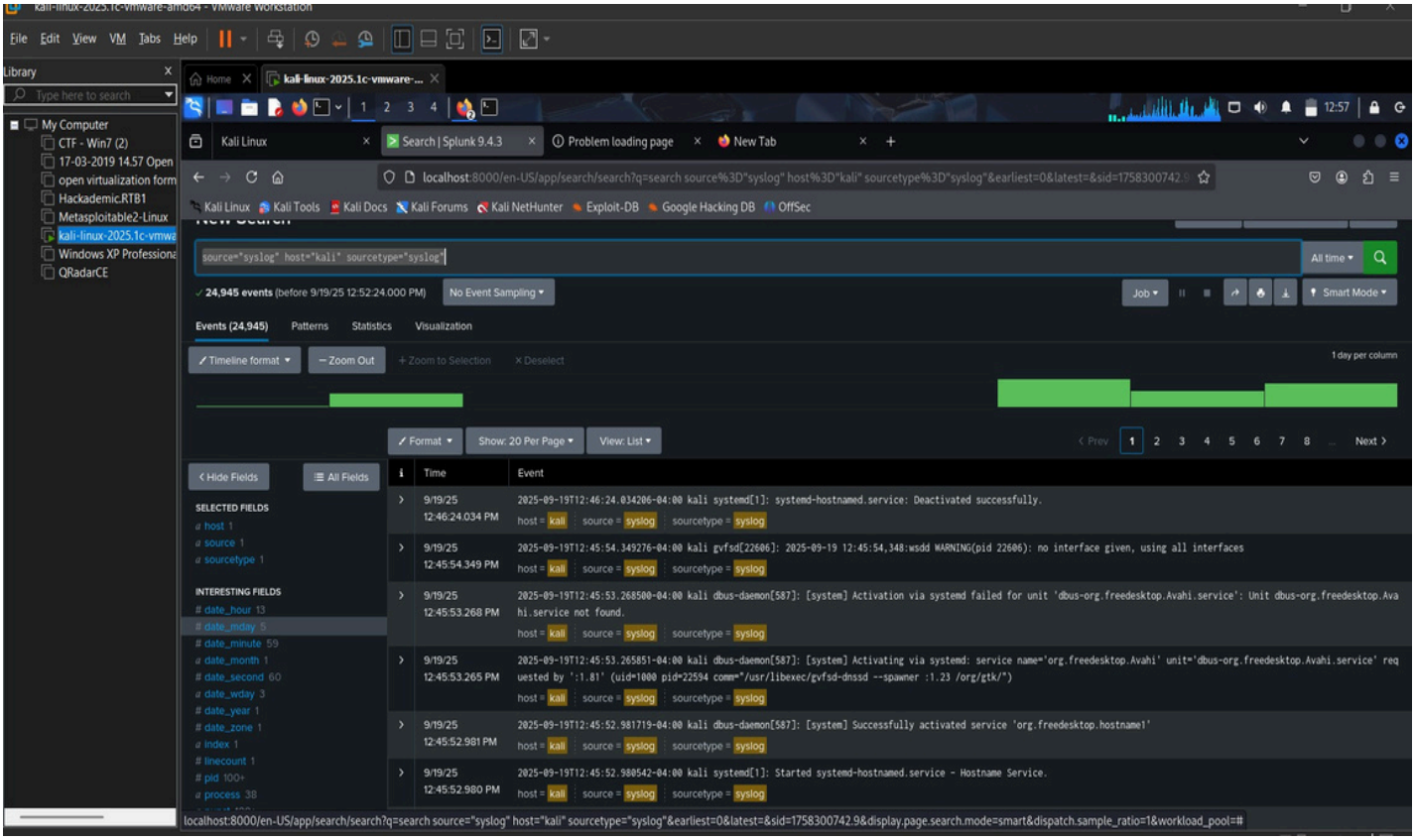
Review and click Submit.



Click on Search.

Run the query: source="syslog" host="kali" sourcetype="syslog"

Splunk displayed the custom log event with timestamp, host, source, and message details.



- I was able to simulate failed login attempts and detect them in Splunk.
- I created a custom log entry using logger and verified its ingestion into Splunk.
- This exercise shows how Splunk can be used for both security monitoring (failed logins) and custom event tracking (logger).