

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.

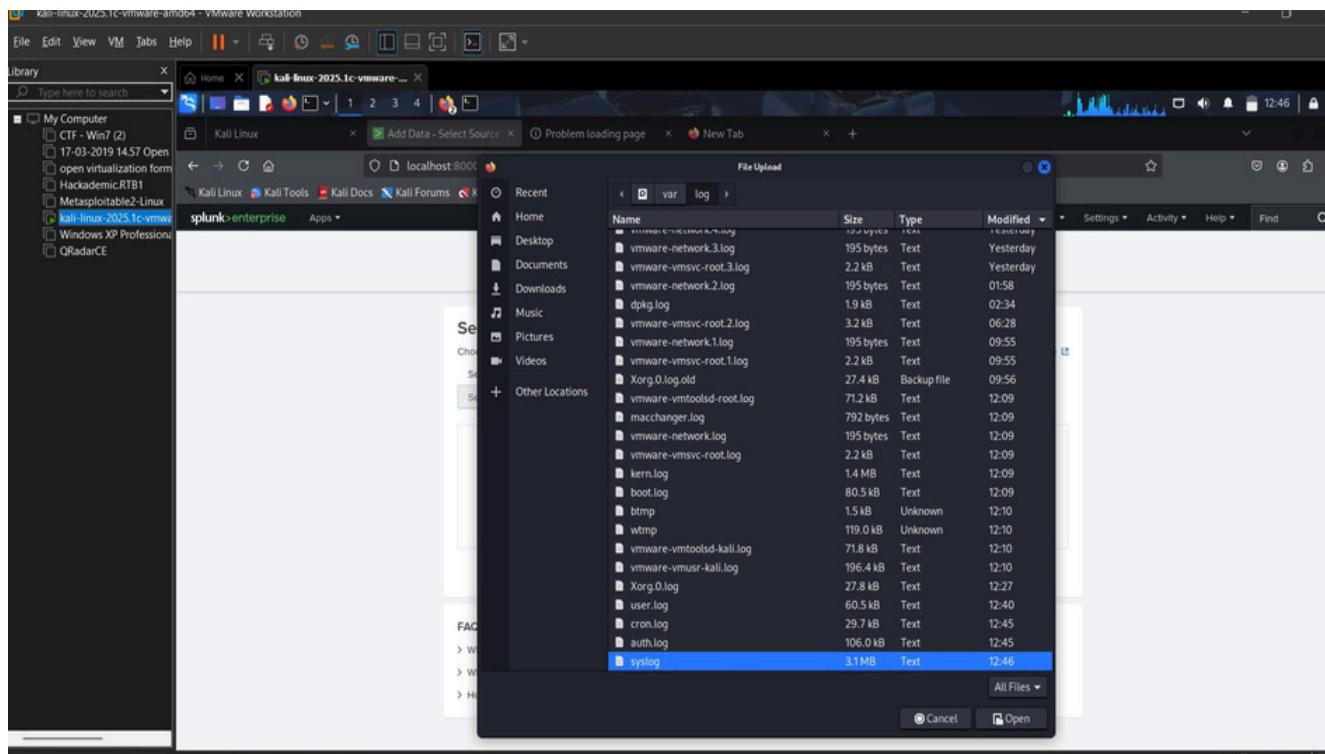
```
(root㉿kali)-[~/home/kali]
# logger "This is a test log from Splunk lab"

(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:

Splunk > enterprise Apps ▾

Add Data Select Source Set Source Type Input Settings Review Done < Back Next >

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: syslog

Source type: syslog ▾ Save As

Event Breaks Timestamp Advanced

Format ▾ Show: 20 Per Page ▾ View: List ▾

	Time	Event
1	9/1/25 6:44:41.081 AM	2025-09-11T06:44:41.081466-04:00 kali rsyslogd: [origin software="rsyslogd" swVersion="8.2504.0" x-pid="589" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
2	9/1/25 6:44:41.112 AM	2025-09-11T06:44:41.112891-04:00 kali systemd[1]: logrotate.service: Deactivated successfully.
3	9/1/25 6:44:41.113 AM	2025-09-11T06:44:41.113131-04:00 kali systemd[1]: Finished logrotate.service - Rotate log files.
4	9/1/25 6:45:03.823 AM	2025-09-11T06:45:03.823789-04:00 kali CRON[4408]: (root) CMD (command -v debian-sal > /dev/null && debian-sal 1 1)
5	9/1/25 6:45:06.967 AM	2025-09-11T06:45:06.967372-04:00 kali systemd[1]: plocate-updatedb.service: Deactivated successfully.
6	9/1/25 6:45:06.969 AM	2025-09-11T06:45:06.969313-04:00 kali systemd[1]: Finished plocate-updatedb.service - Update the plocate database.
7	9/1/25 6:45:06.970 AM	2025-09-11T06:45:06.970657-04:00 kali systemd[1]: plocate-updatedb.service: Consumed 10.719s CPU time, 318.9M memory peak, 41.1M memory swap peak.
8	9/1/25 6:45:06.974 AM	2025-09-11T06:45:06.974274-04:00 kali systemd[1]: Starting apt-daily.service - Daily apt download activities...

View Event Summary < Prev 1 2 3 4 5 6 7 8 ... Next >

Review and click Submit.

Add Data Select Source Set Source Type Input Settings Review Done < Back Submit >

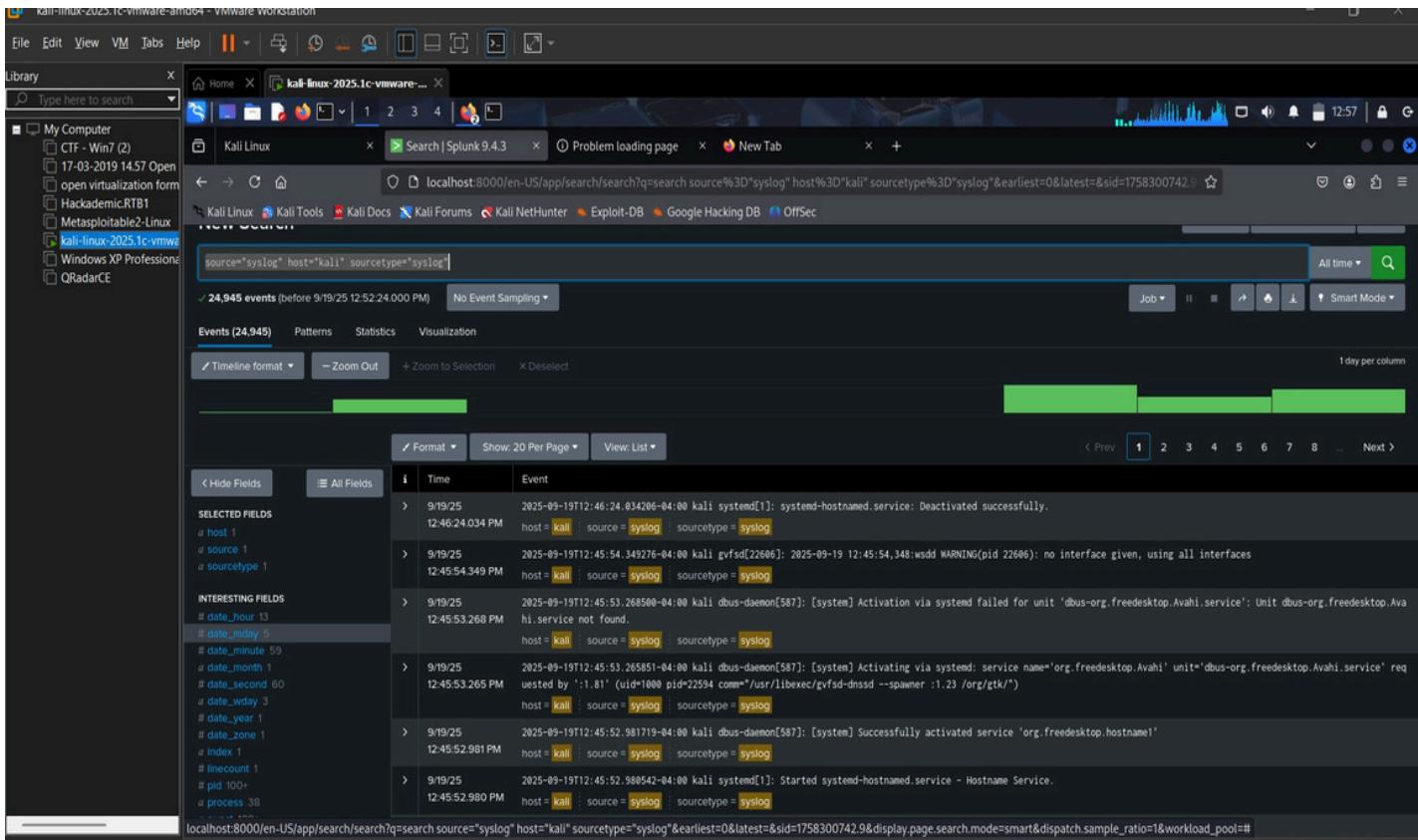
Review

Input Type Uploaded File
File Name syslog
Source Type syslog
Host kali
Index Default

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).