Phase 2: Log Integration and SIEM Analysis

SIEM Configuration and Environment Setup

In this phase, the goal was to integrate and analyze security logs from both the attacker and victim environments using Splunk.

- **SIEM Platform**: Splunk Enterprise, installed locally on a Windows machine.
- **Attacker Machine**: Kali Linux (used to launch the SSH brute-force attack).
- **Victim Machine**: Metasploitable 3 (running on VirtualBox).

To collect and analyze attack data in Splunk, the authentication was manually extracted and transferred to the Splunk server hosted on a Windows machine.

1. Log File Preparation on Kali

The log file /var/log/auth.log was located and confirmed to contain SSH login activity, including failed and successful attempts related to the brute-force attack conducted in Phase 1.

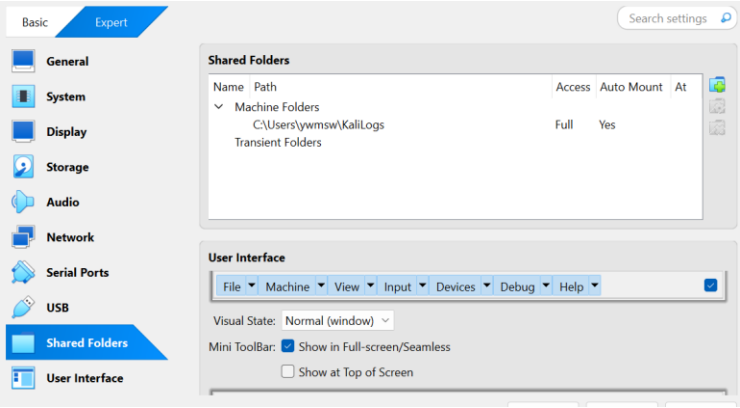
It was then copied to the home directory for export:

sudo cp /var/log/auth.log

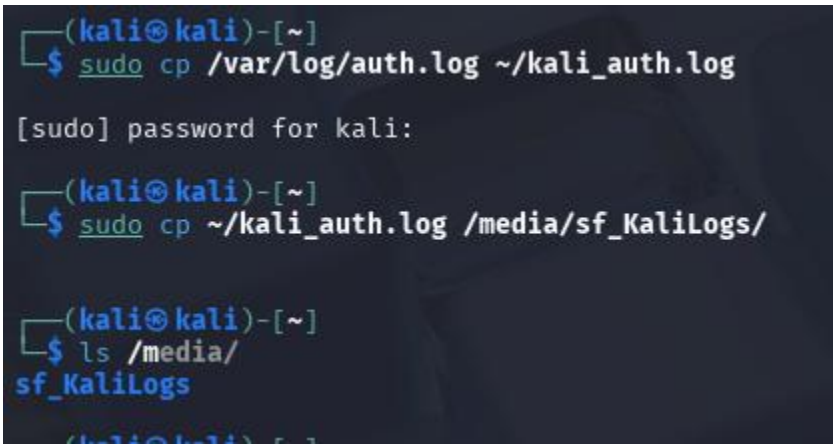
2. File Transfer from Kali to Windows

To move the log file to the Windows system running Splunk, a shared folder was configured between the Kali VM and the host machine:

- **Shared Folder Path on Windows**: C:\Users\ywmsw\KaliLogs



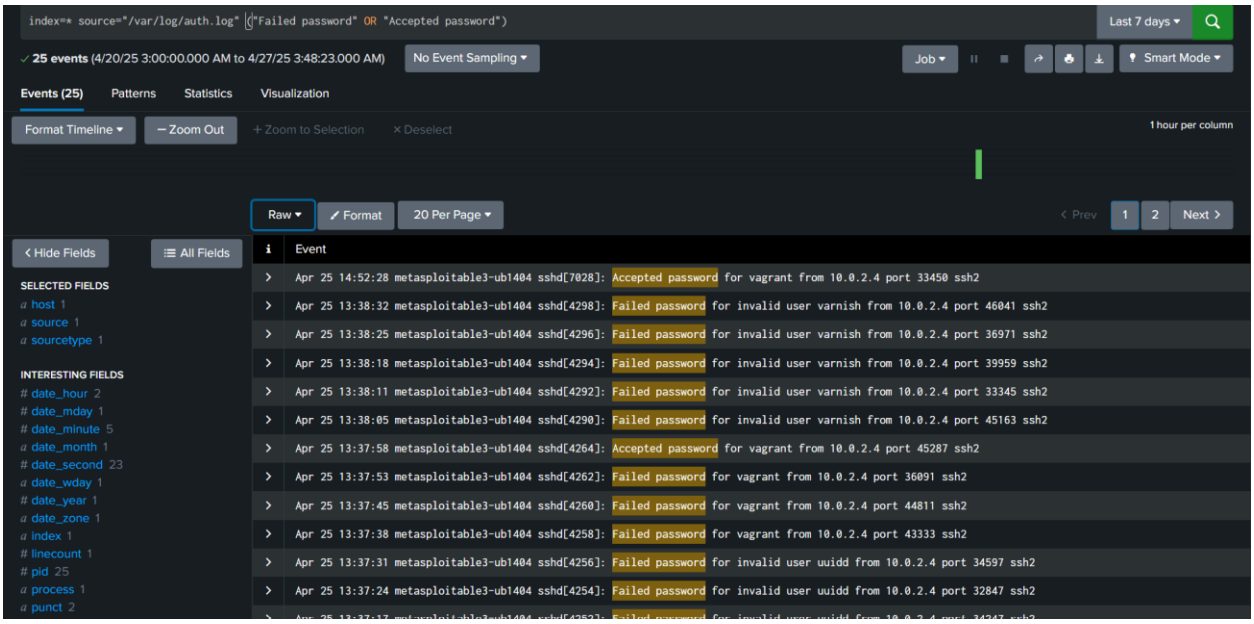
the shared folder was visible under /media/sf_KaliLogs. The log file was copied into it using:



Log Visualization and Attack Analysis

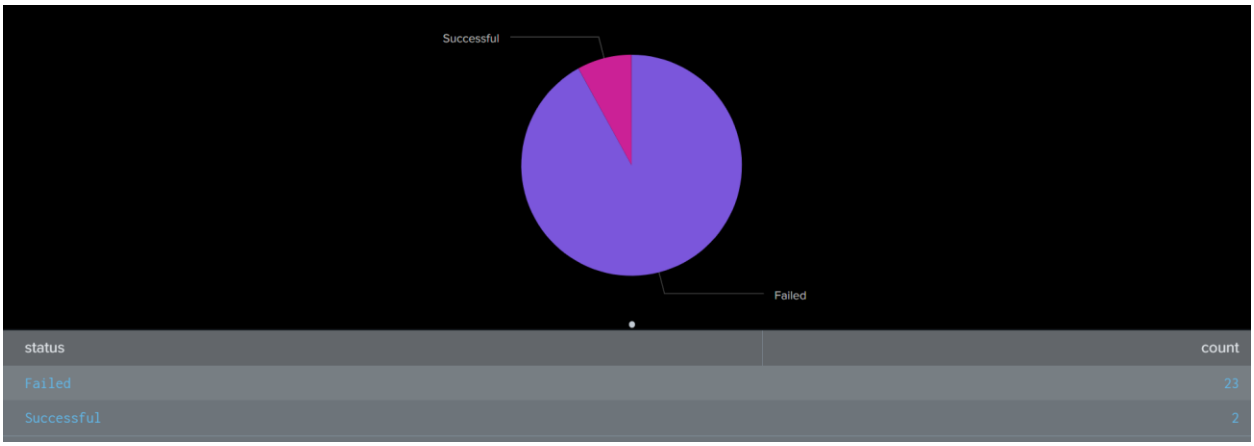
Splunk's search and visualization tools were used to investigate the logs and better understand the attack behavior.

Raw Log View



These logs display SSH login attempts from the attacker, highlighting both rejected and accepted credentials.

Success vs Failure (Pie Chart)



status	count
Failed	23
Successful	2

- Among all SSH login attempts, the majority failed.
- Only **2 login attempts** succeeded, while **23 attempts** were rejected.
- This behavior is consistent with brute-force attacks where many incorrect guesses eventually uncover valid credentials — emphasizing the risk of using weak or common passwords.

Comparative Insights: Attacker vs Victim Logs

After aligning logs from both systems:

- The victim's system captured a series of failed and successful SSH attempts, consistent with a brute-force pattern.
- The attack timestamps and source IP address matched the activity recorded on the Kali attacker machine.
- This confirmed a **direct correlation** between the attacks and the logs — proving the compromise and allowing full traceability of the breach.