# Task 2 – Security Alert Monitoring & Incident Response Report

## 1. Executive Summary

This report summarizes the findings from Task 2 of the Future Interns Cyber Security Internship. The task involved analyzing simulated security alerts using Splunk and documenting incidents such as malware detection, authentication failures, and suspicious connections. The objective was to simulate the role of a SOC analyst in identifying, classifying, and responding to potential threats.

## 2. Tools Used

- Splunk (local installation on Kali Linux)  
- SOC\_Task2\_Sample\_Logs.txt  
- Kali Linux VM  
- Web Browser (Firefox)

## 3. Log Analysis & Search Queries

The following Splunk search queries were used to identify key security incidents:

source="SOC\_Task2\_Sample\_Logs.txt" (malware OR "Trojan Detected" OR "Rootkit Signature" OR "Spyware Alert" OR "Worm Infection Attempt" OR "Ransomware Behavior")

source="SOC\_Task2\_Sample\_Logs.txt" ("login failed" OR "Failed login" OR "Failed password" OR "authentication failure")

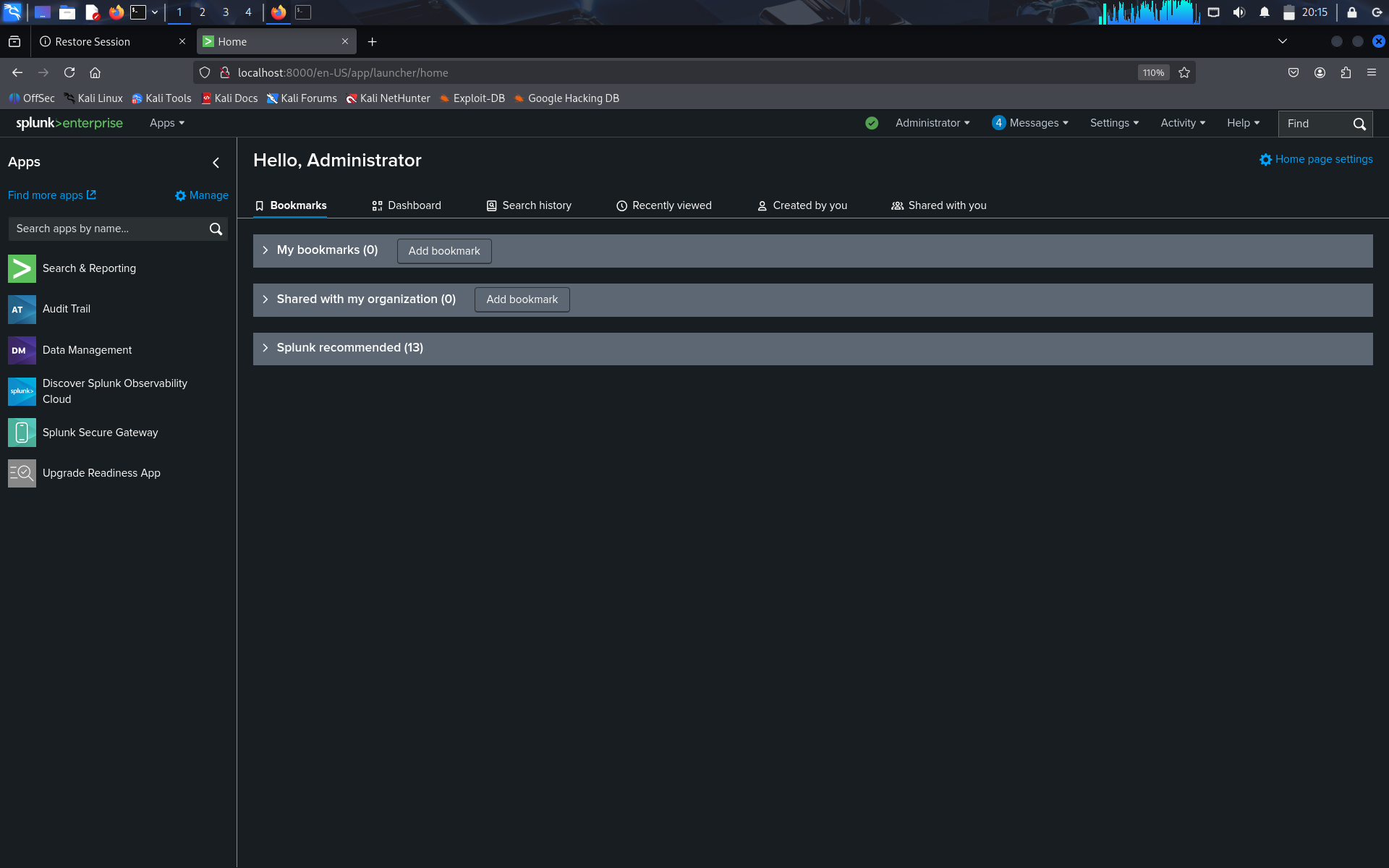
source="SOC\_Task2\_Sample\_Logs.txt" "connection attempt" OR "unauthorized connection"

source="SOC\_Task2\_Sample\_Logs.txt" | stats count by user

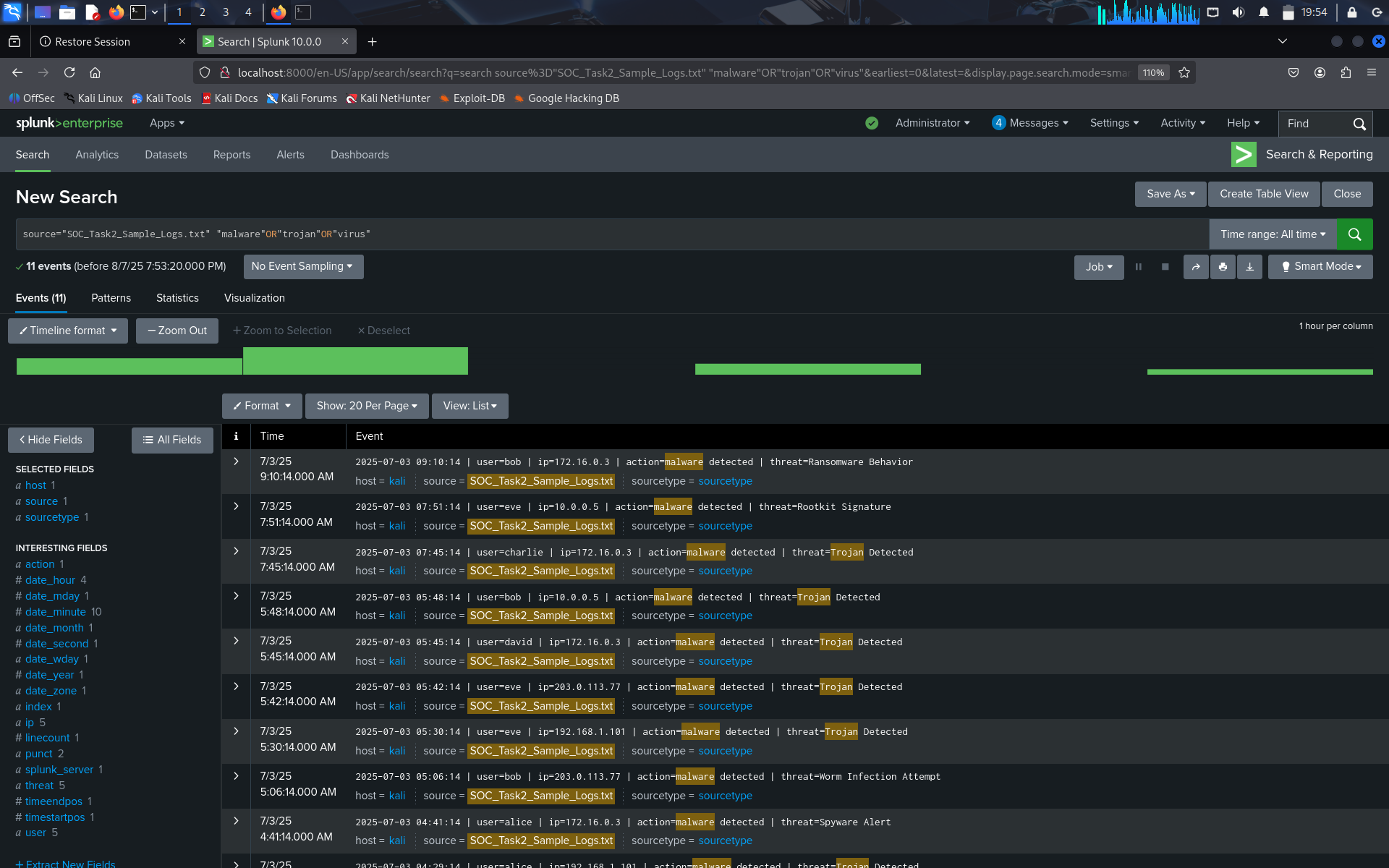
## 4. Screenshots & Findings

Below are the visual outputs and key findings from each query run in Splunk.

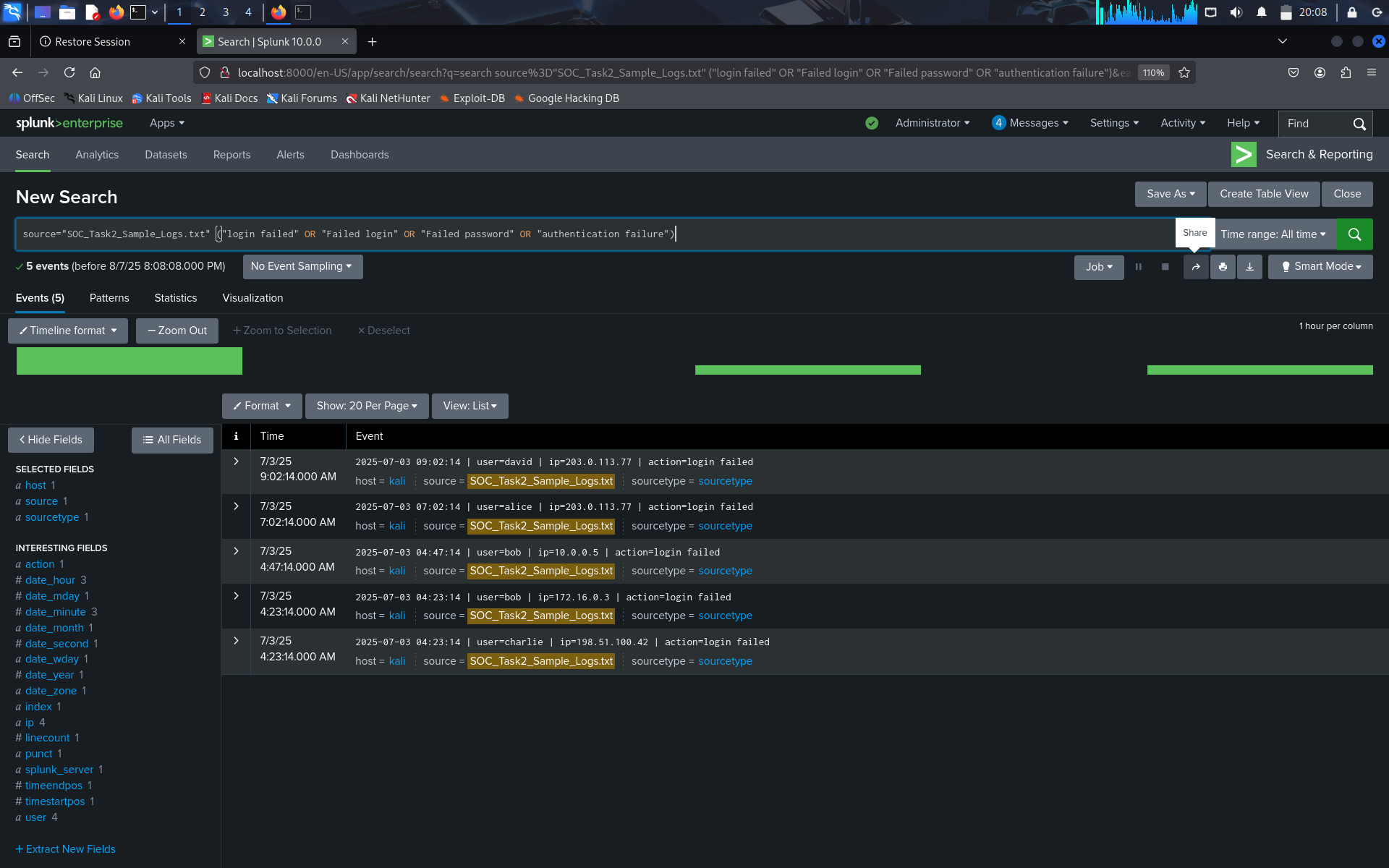
### Splunk Home Page



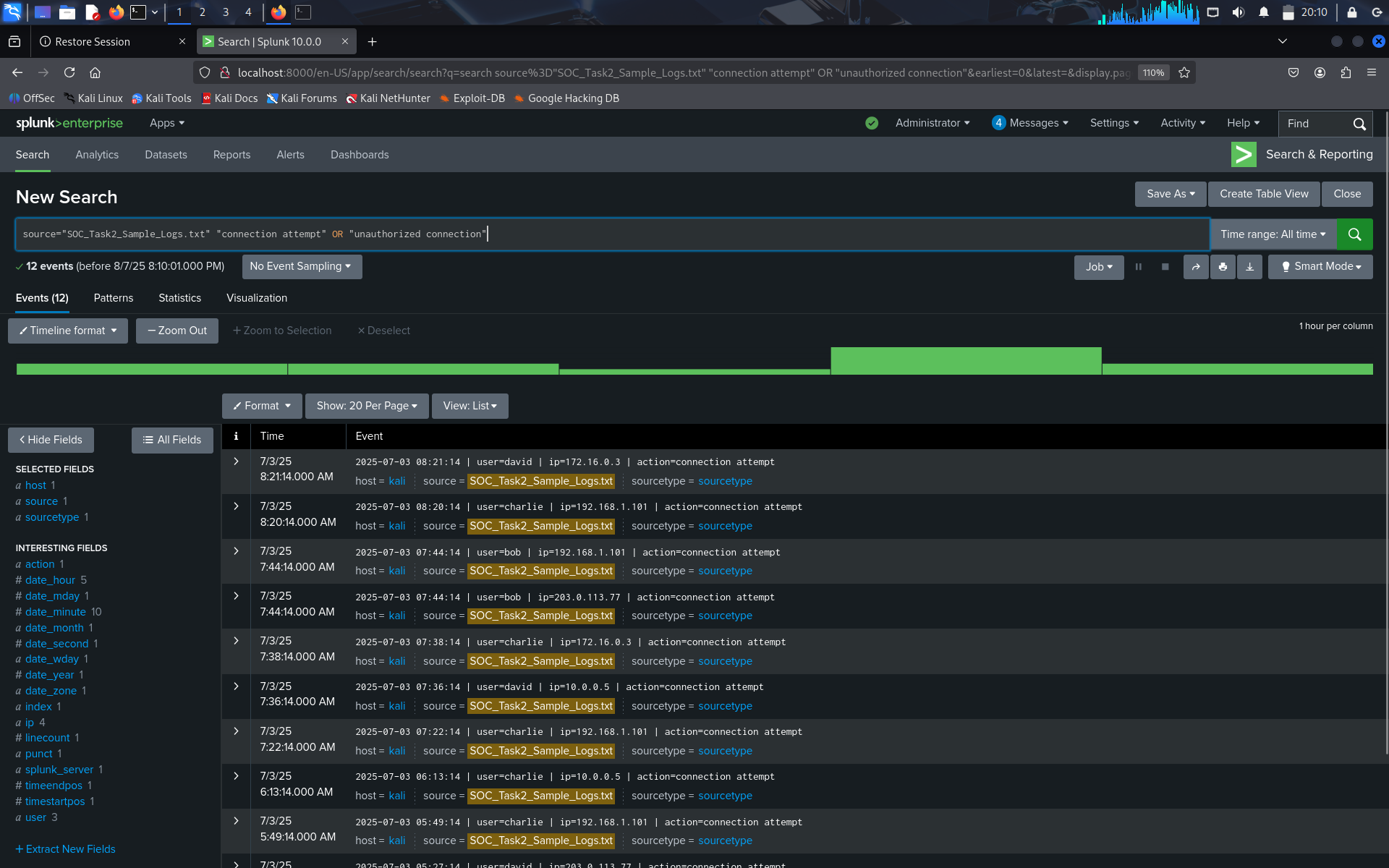
### Malware Alerts Query Result



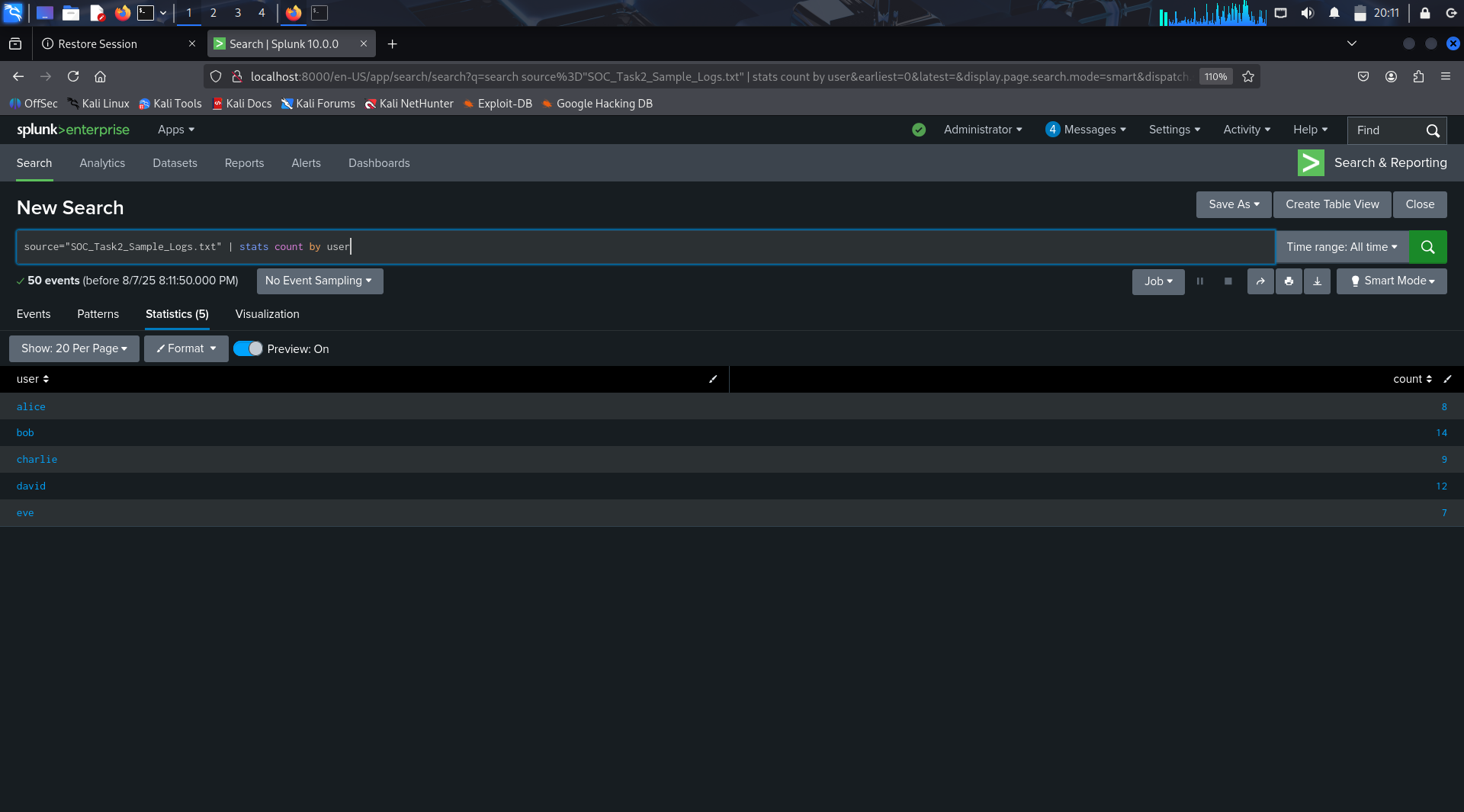
### Login Failures Query Result



### Suspicious Connection Attempts



### User Behavior Stats



## 5. Incident Summary Table

A summary of major incidents identified from the log analysis is provided below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Alert Type | User | Source IP | Time | Description |
| Malware Detected | bob | 10.0.0.5 | 2025-07-03 05:48:14 | Trojan activity detected on internal host |
| Login Failure | alice | 203.0.113.77 | 2025-07-03 07:02:14 | Multiple failed login attempts |
| Suspicious Connection | david | 203.0.113.77 | 2025-07-03 06:10:14 | Unauthorized repeated connection attempts |
| Rootkit Signature | eve | 10.0.0.5 | 2025-07-03 07:51:14 | Detected rootkit signature on critical system |

## 6. Recommendations

- Immediately isolate systems affected by malware for cleanup  
- Enforce multi-factor authentication for all user accounts  
- Block repeated failed login attempts via firewall or intrusion detection rules  
- Conduct thorough endpoint security review and patch known vulnerabilities

## 7. Conclusion

This exercise helped simulate a real-world SOC (Security Operations Center) workflow. By leveraging Splunk and simulated logs, we were able to identify threats, understand user behavior patterns, and recommend actions for remediation. The hands-on task improved threat detection and response skills significantly.