DHANARAJ PATIL

FUTURE_CS_02 - Task 2: SOC Internship - Security Alert Monitoring & Incident Response Simulation

➢ Task Overview

This task simulated the role of a SOC analyst handling security events. I configured and used a SIEM solution (Splunk) to detect abnormal activities like unauthorized access, brute force attempts, and malware infections. Logs were analysed, alerts prioritized, and incident reports drafted.

➢ Tools & Technologies

- Splunk
- Kali Linux
- Sample Log Datasets
- GitHub markdown for documentation
- MS Word for incident reports

➢ Key Activities:

- SIEM setup and Real-time log analysis with Splunk - Alert analysis (failed logins, malware, suspicious IPs)
- Detection of malware (Trojan, Rootkit) - Connection attempt monitoring - Alert severity classification

➢ Summary

Multiple malware alerts and repeated authentication failures were identified across several internal user accounts and IP addresses. Public IP addresses were involved in both login activity and malware detections, suggesting the possibility of remote compromise and lateral movement.

➢ Key Findings

Event Type	Description	Affected Users	Impacted IPs
Malware Detected	Various signatures including Trojan, Ransomware	bob, alice, david, eve	198.51.100.42, 10.0.0.5
Login Failures	Repeated failures from external IPs	bob, alice, david, charlie	203.0.113.77, 198.51.100.42
Suspicious Access	File access following malware detections	bob, david, eve	Mixed internal + external

➢ Alerts & Prioritization

Alert Type	Severity	Justification
Trojan Detected (multi-user)	High	Widespread infection observed across internal users
Ransomware Behavior	Critical	Flagged on user bob; potential data encryption detected
Rootkit Signature	High	Advanced threat; observed on eve, alice
Login Failures from Public IP	Medium	Possible brute-force or credential stuffing attempt
File Access Post-Infection	Medium	Indicates possible data exfiltration

---

➢ Event Timeline

Timestamp	User	IP Address	Activity
04:18–04:41	alice	Multiple	Malware detection + file access
05:06	bob	203.0.113.77	Worm Infection Attempt
06:21	alice	203.0.113.77	Login success after infection
07:45	charlie	172.16.0.3	Trojan alert
09:10	bob	172.16.0.3	Ransomware behavior

➢ Incident Response Recommendations

- **Mitigation**
  - Isolate impacted systems immediately.
  - Disable user accounts for bob, alice, charlie, david, and eve.
  - Initiate malware scans and forensic review.
- **Investigation**
  - Correlate login timestamps with malware alert windows.
  - Identify if infected users accessed sensitive resources or executed binaries.
- **Containment & Remediation**
  - Block suspicious public IPs: 203.0.113.77, 198.51.100.42
  - Deploy network segmentation for vulnerable zones.
  - Patch known exploits and review endpoint configurations.

➢ Next Steps

- Enable threat intelligence and geolocation enrichment in Splunk.
- Configure correlation searches for multi-stage attack detection.
- Build dashboards for real-time malware and login anomaly alerts.

➢ Incident Response Simulation

Scenario:

Over a 5-hour window on July 3rd, 2025, malware detections (Trojan, Rootkit, Ransomware) occurred across internal users and IPs. These alerts were paired with failed logins, suspicious external IP activity, and anomalous file access patterns—suggesting coordinated compromise attempts with possible lateral movement.

Detected Activities:

Malware alerts from 5 user accounts - Login failures from suspicious external IPs - File access following infection - Ransomware signatures on user bob

Actions Taken:

User sessions isolated - IP access blocked - Alerts escalated and enriched - Response report compiled and dashboard built for visibility

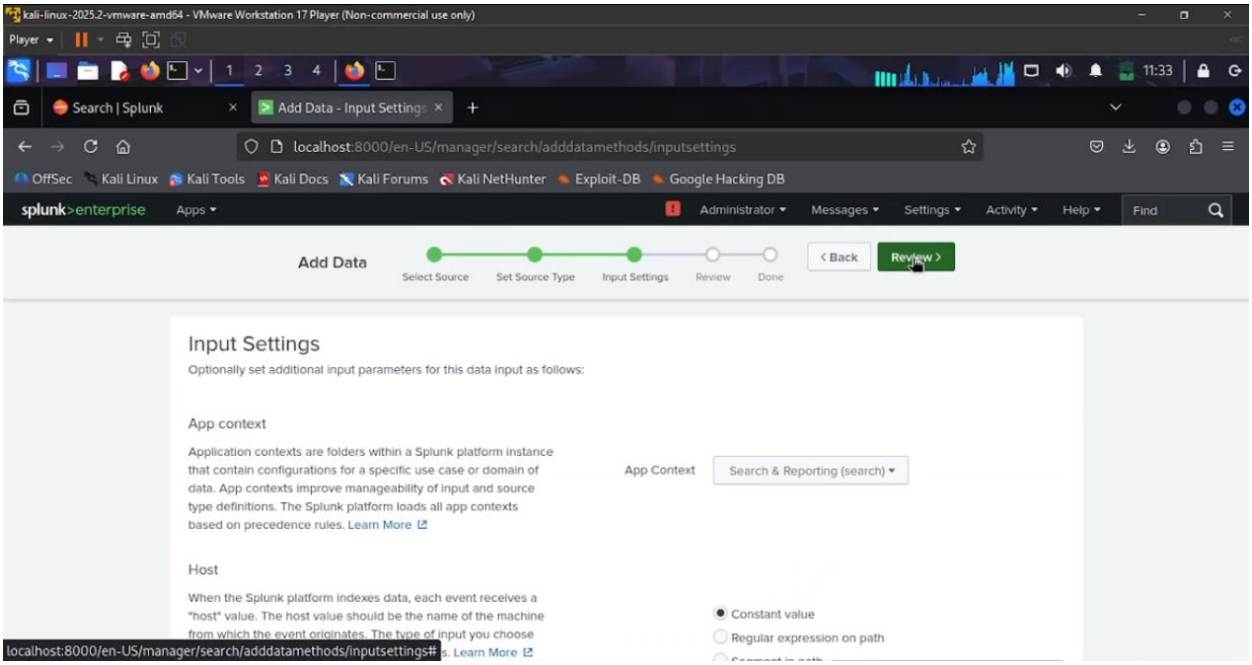
➢ SOC Playbook Implementation

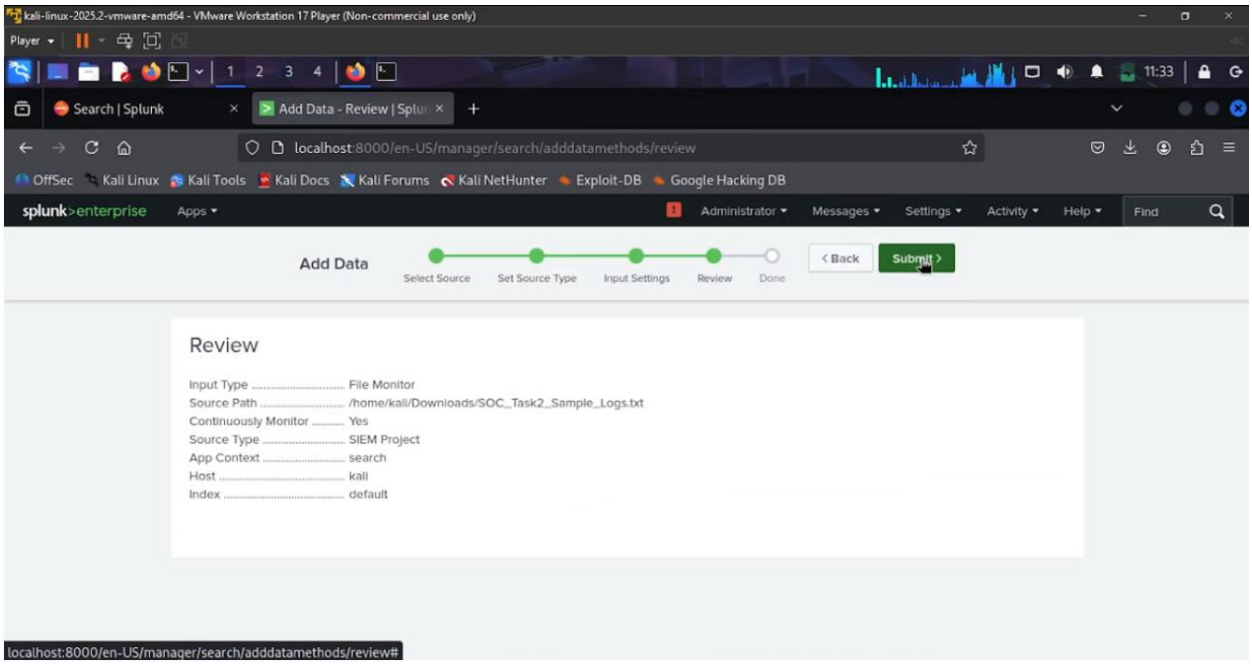
Step	Action
Detection	SPL searches flagged malware, failed logins, file access anomalies
Triage	Categorized alerts by severity and user risk
Investigation	Correlated events across time, user, and IPs to uncover attack vectors
Containment	Suggested isolation of infected hosts and user accounts
Remediation	Malware scan initiated, user permissions revoked
Recovery & Monitoring	Real-time dashboard deployed, external IP alerts configured
Documentation	Report filed (see below), queries saved, timeline logged

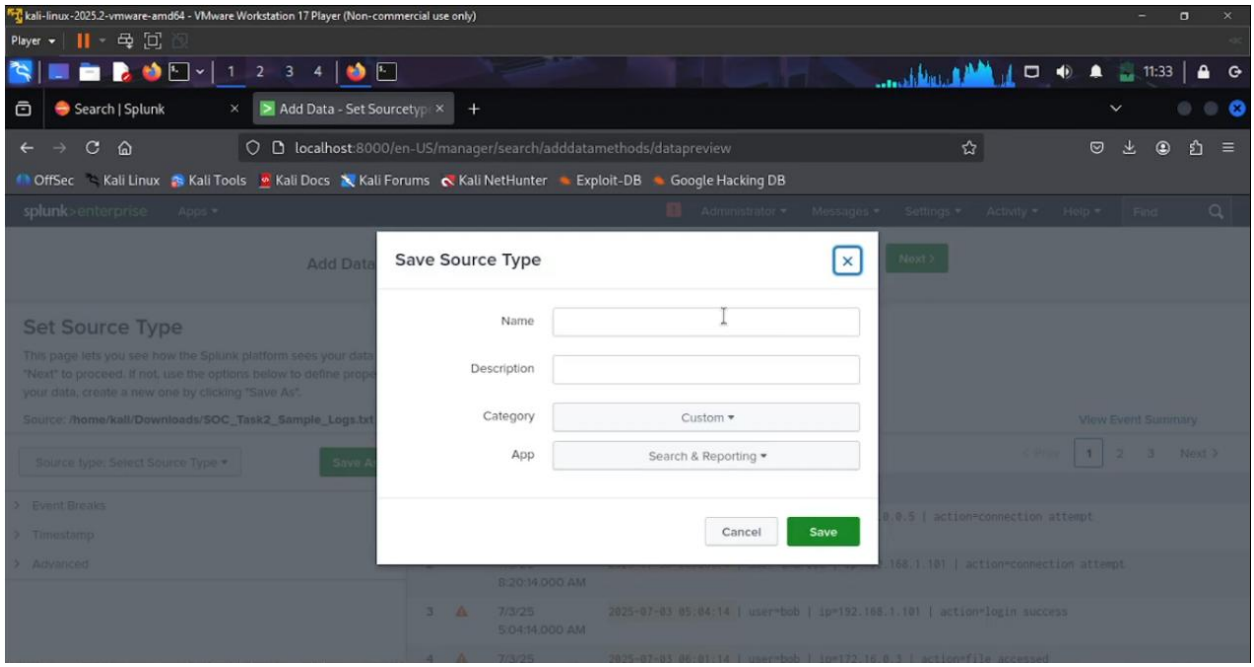
➢ SOC Dashboard Metrics

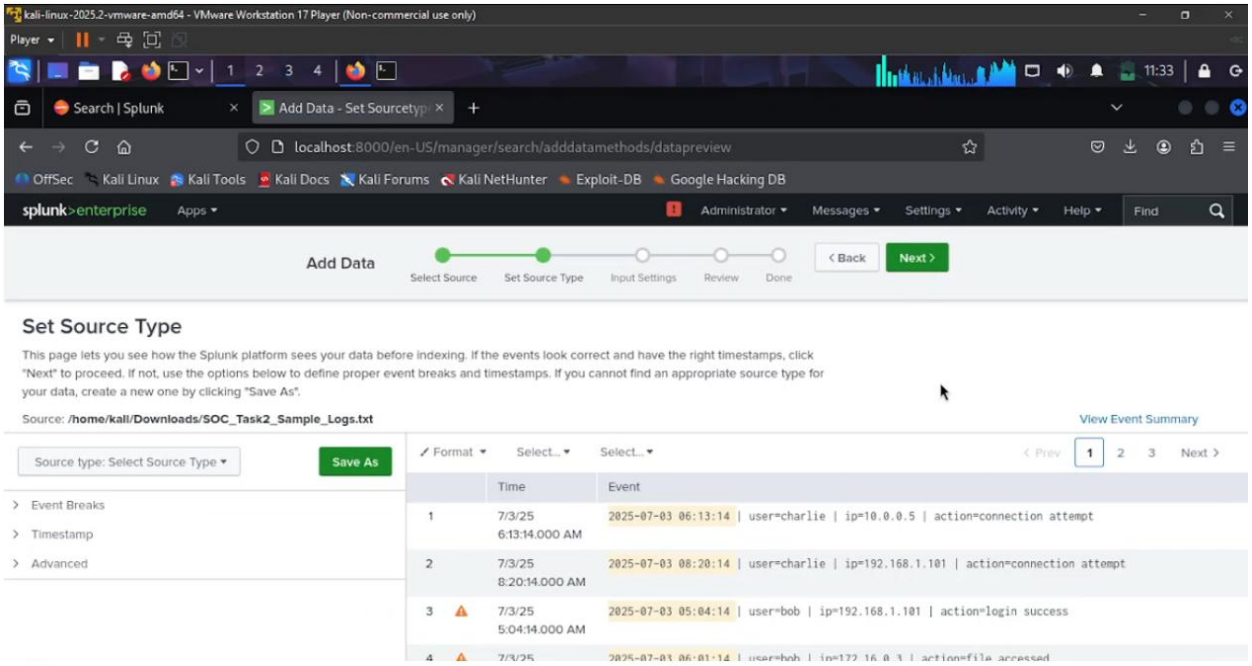
Panel Title	Description	Example Visualization
Malware Alerts by Signature	Counts of Trojan, Rootkit, etc. per user	Bar Chart
Failed Logins Heatmap	Auth failure frequency per hour per user	Heatmap
External IP Access	Attempts from flagged IPs	Table + Severity Tags
Incident Timeline	All alert types across time	Time Series Line Chart
Severity Breakdown	Alert counts by High/Medium/Low classification	Pie or Donut Chart

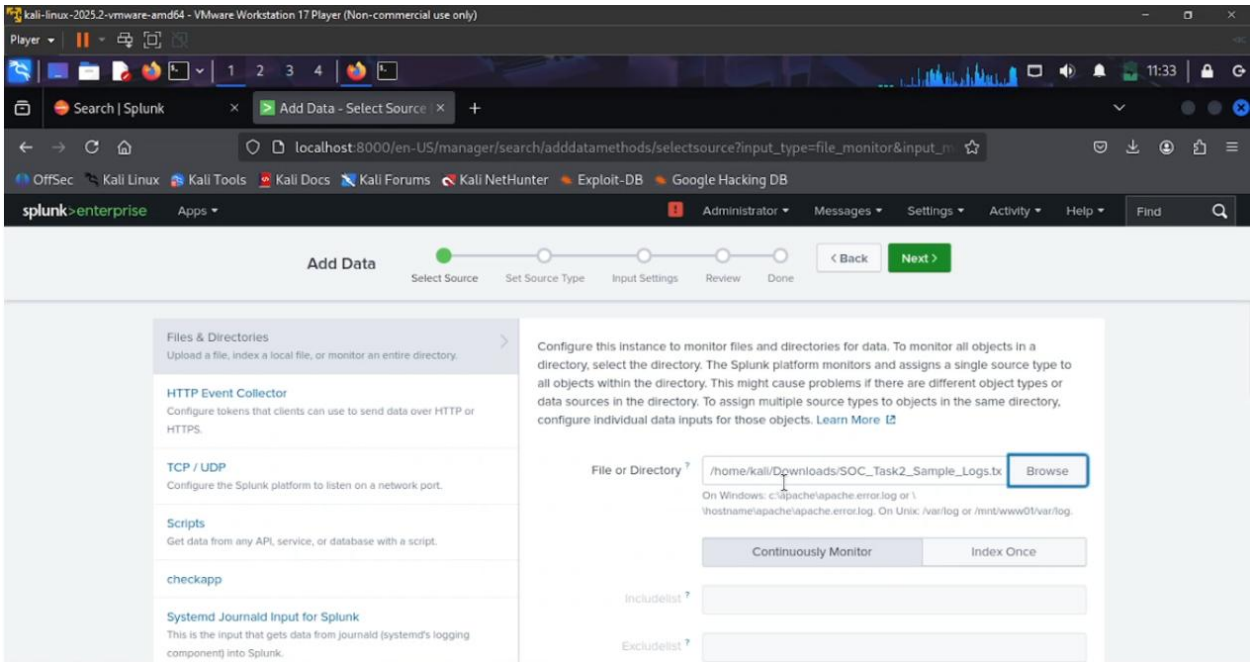
➢ Attachments:

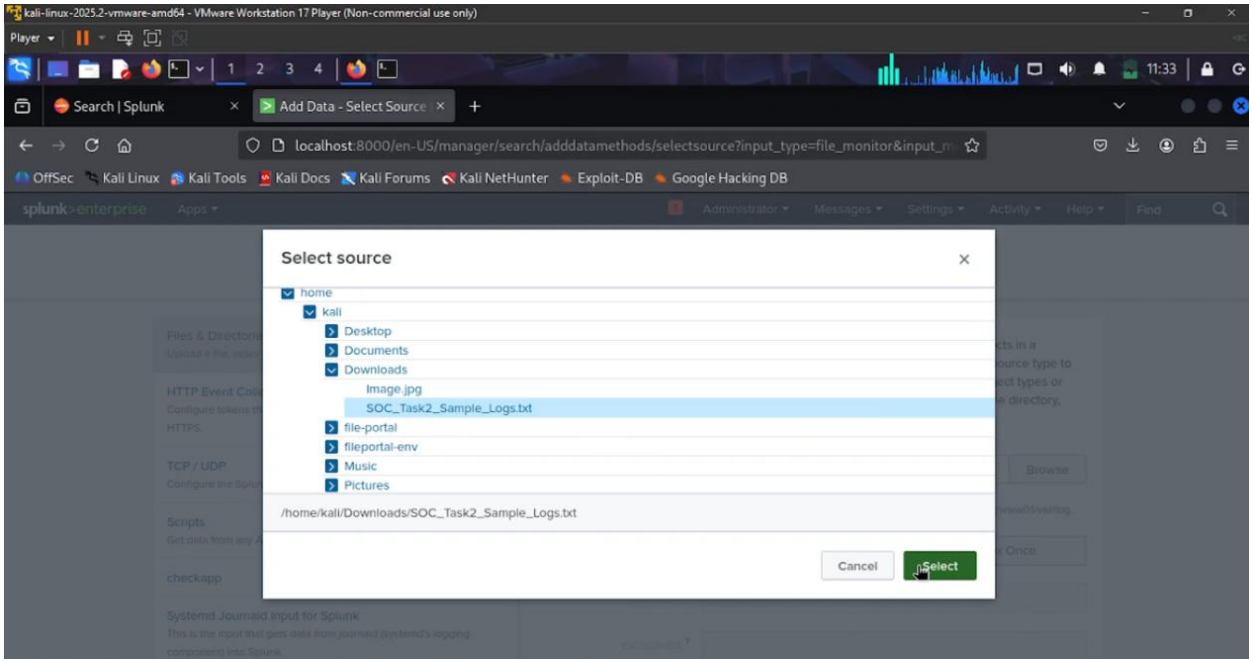


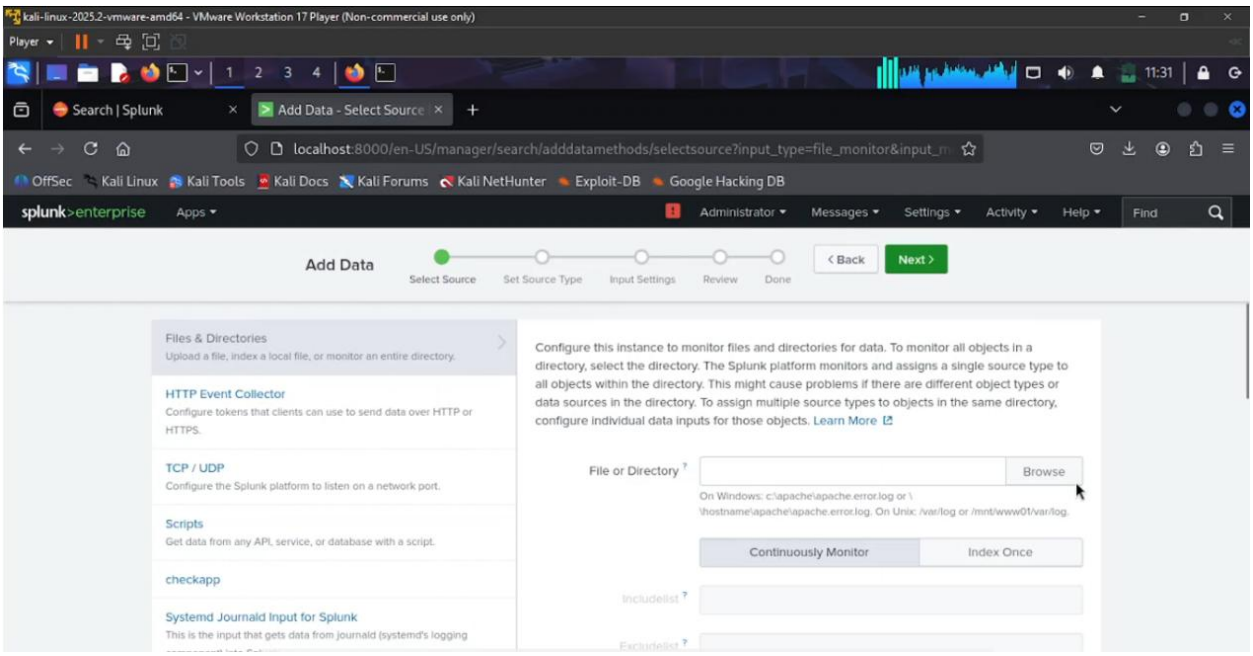


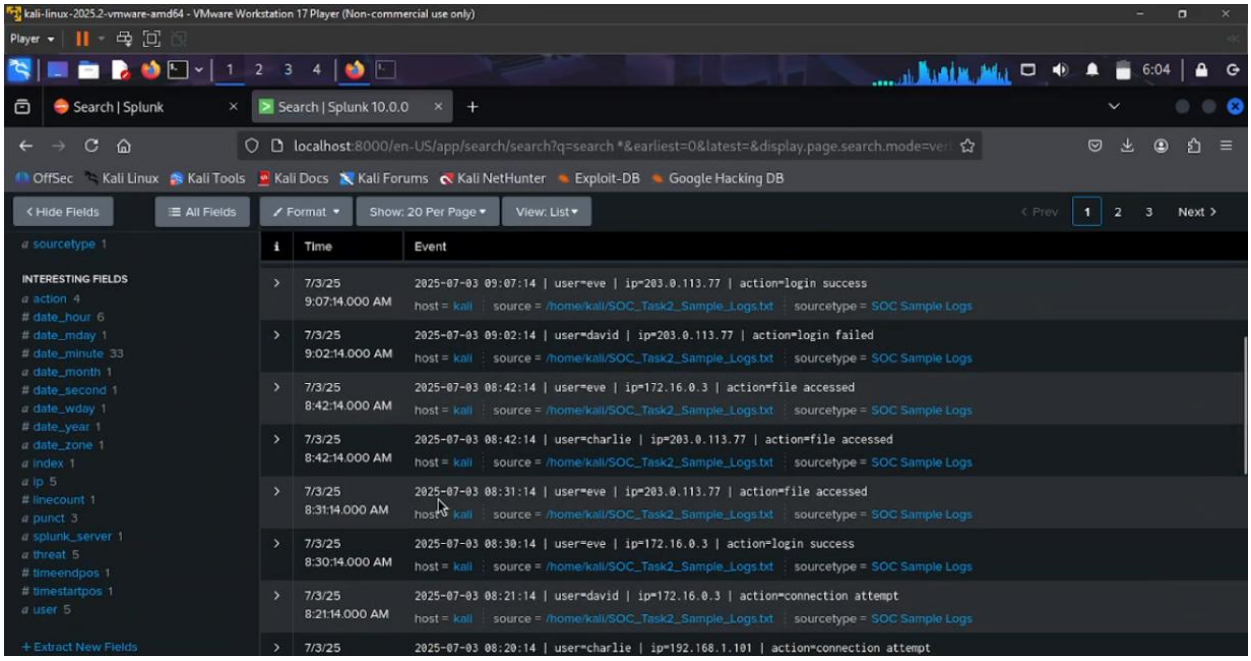

kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk
Add Data - Set Sourcetyp
localhost:8000/en-US/manager/search/adddatamethods/datapreview
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Next >
Set Source Type
Source: /home/kali/Downloads/SOC_Task2_Sample_Logs.txt
Source type: Select Source Type
Save As
Event Breaks
Timestamp
Advanced
View Event Summary
Save Source Type
Name
Description
Category
Custom
App
Search & Reporting
Cancel
Save

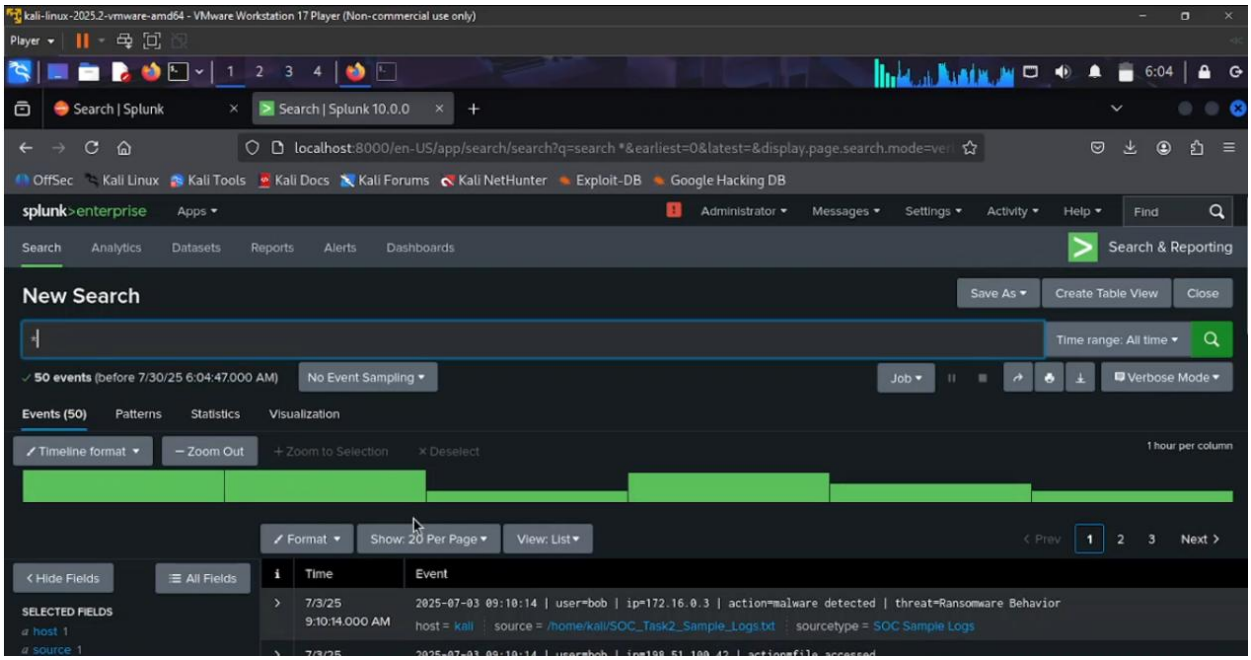

kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk
Add Data - Set Sourcetyp
localhost:8000/en-US/manager/search/adddatamethods/datapreview
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
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: /home/kali/Downloads/SOC_Task2_Sample_Logs.txt
View Event Summary
Source type: Select Source Type
Save As
Format
Select...
Select...
< Prev
1
2
3
Next >
Event Breaks
Timestamp
Advanced
Time
Event
1
7/3/25 6:13:14.000 AM
2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2
7/3/25 8:20:14.000 AM
2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
3
7/3/25 5:04:14.000 AM
2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success

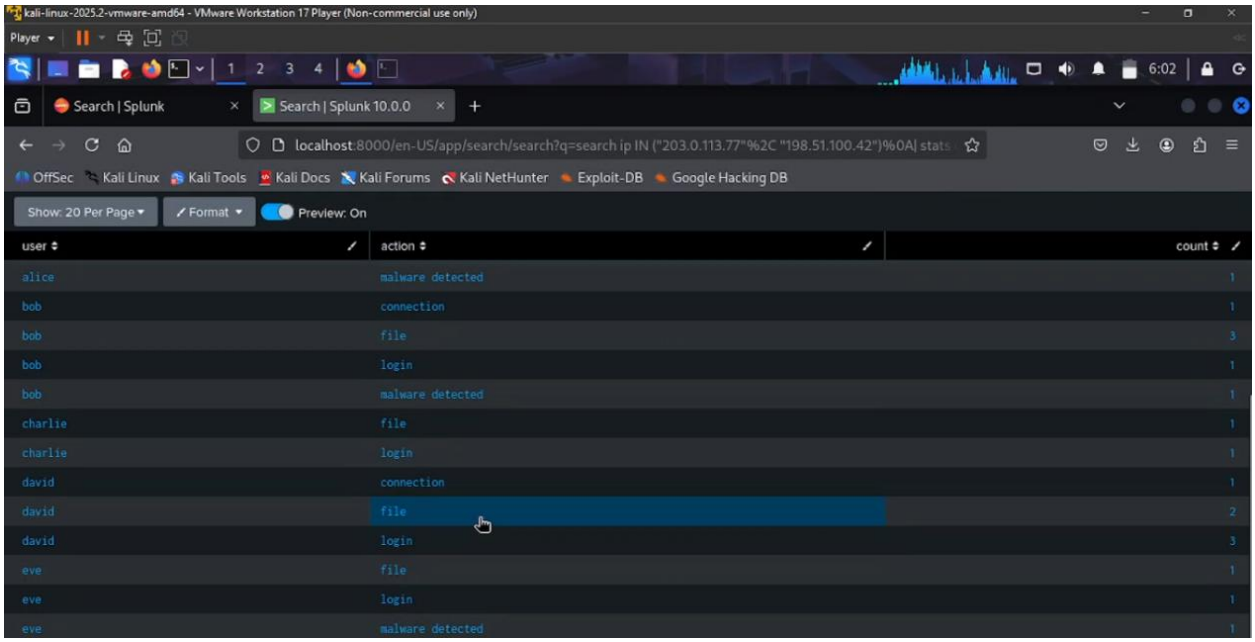

kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk
Add Data - Select Source
localhost:8000/en-US/manager/search/adddatamethods/selectsource?input_type=file_monitor&input_m
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
splunk>enterprise Apps Administrator Messages Settings Activity Help Find
Add Data
Select Source Set Source Type Input Settings Review Done
Back Next
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure the Splunk platform to listen on a network port.
Scripts
Get data from any API, service, or database with a script.
checkapp
Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.
Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More
File or Directory
/home/kali/Downloads/SOC_Task2_Sample_Logs.tx
Browse
Continuously Monitor
Index Once
Includelist
Excludelist

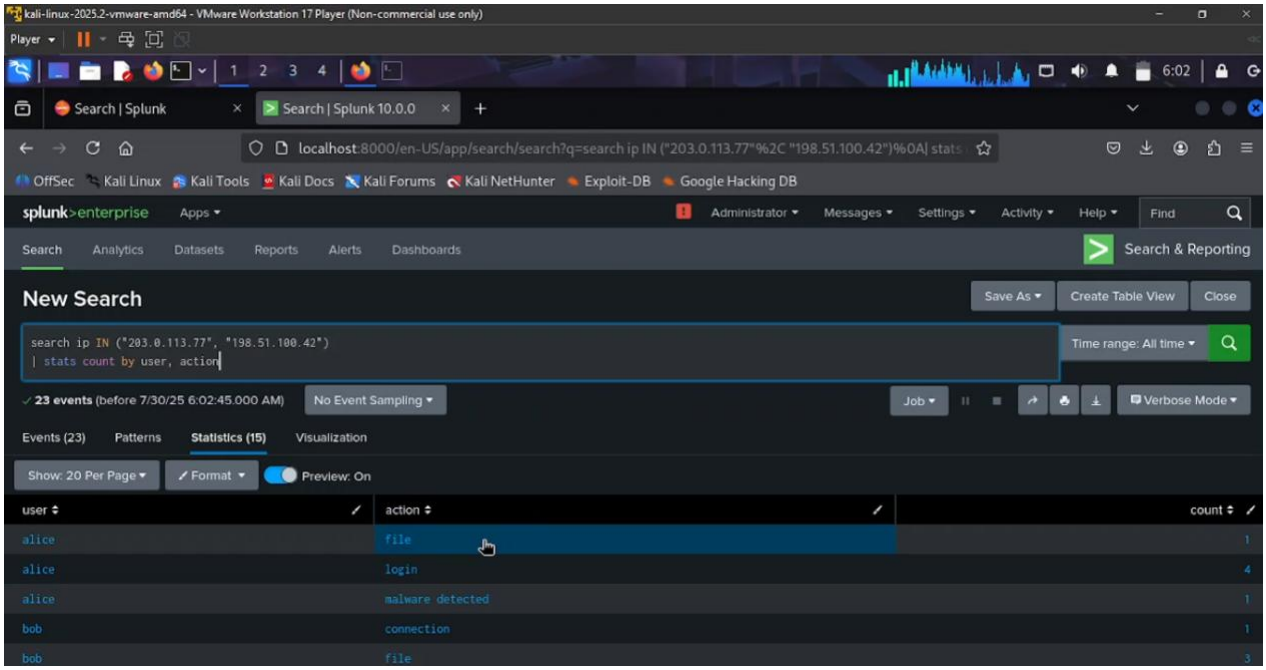

kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk
Add Data - Select Source
localhost:8000/en-US/manager/search/adddatamethods/selectsource?input_type=file_monitor&input_m
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Select source
home
kali
Desktop
Documents
Downloads
Image.jpg
SOC_Task2_Sample_Logs.txt
file-portal
fileportal-env
Music
Pictures
/home/kali/Downloads/SOC_Task2_Sample_Logs.txt
Cancel
Select

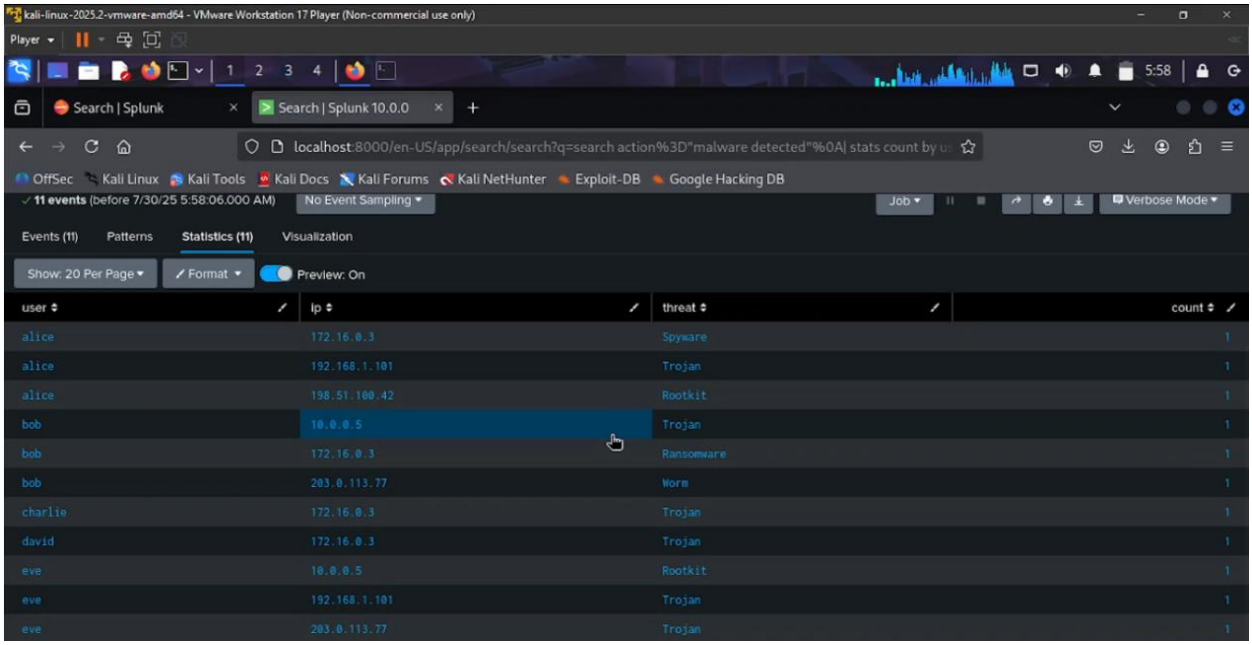

kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk
Add Data - Select Source
localhost:8000/en-US/manager/search/adddatamethods/selectsource?input_type=file_monitor&input_m
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
splunk>enterprise Apps Administrator Messages Settings Activity Help Find
Add Data
Select Source Set Source Type Input Settings Review Done
Back Next
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure the Splunk platform to listen on a network port.
Scripts
Get data from any API, service, or database with a script.
checkapp
Systemd Journald Input for Splunk
Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More
File or Directory
Browse
On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.
Continuously Monitor
Index Once


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk
Search | Splunk 10.0.0
localhost:8000/en-US/app/search/search?q=search *&earliest=0&latest=&display.page.search.mode=ver
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Hide Fields All Fields Format Show: 20 Per Page View: List
Prev 1 2 3 Next
sourcetype 1
INTERESTING FIELDS
action 4
date_hour 6
date_mday 1
date_minute 33
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
index 1
ip 5
linecount 1
punct 3
splunk_server 1
threat 5
timeendpos 1
timestartpos 1
user 5
Extract New Fields
Time
Event
7/3/25 9:07:14.000 AM 2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success host = kali source = /home/kali/SOC_Task2_Sample_Logs.txt sourcetype = SOC Sample Logs
7/3/25 9:02:14.000 AM 2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed host = kali source = /home/kali/SOC_Task2_Sample_Logs.txt sourcetype = SOC Sample Logs
7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed host = kali source = /home/kali/SOC_Task2_Sample_Logs.txt sourcetype = SOC Sample Logs
7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed host = kali source = /home/kali/SOC_Task2_Sample_Logs.txt sourcetype = SOC Sample Logs
7/3/25 8:31:14.000 AM 2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed host = kali source = /home/kali/SOC_Task2_Sample_Logs.txt sourcetype = SOC Sample Logs
7/3/25 8:30:14.000 AM 2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success host = kali source = /home/kali/SOC_Task2_Sample_Logs.txt sourcetype = SOC Sample Logs
7/3/25 8:21:14.000 AM 2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt host = kali source = /home/kali/SOC_Task2_Sample_Logs.txt sourcetype = SOC Sample Logs
7/3/25 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk
Search | Splunk 10.0.0
localhost:8000/en-US/app/search/search?q=search *&earliest=0&latest=&display.page.search.mode=ver
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
splunk>enterprise Apps Administrator Messages Settings Activity Help Find
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Save As Create Table View Close
Time range: All time
50 events (before 7/30/25 6:04:47.000 AM) No Event Sampling Job Verbose Mode
Events (50) Patterns Statistics Visualization
Timeline format Zoom Out Zoom to Selection Deselect
1 hour per column
Format Show: 20 Per Page View: List
Prev 1 2 3 Next
Hide Fields All Fields
SELECTED FIELDS
host 1
source 1
Time Event
7/3/25 9:10:14.000 AM
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
host = kali source = /home/kali/SOC_Task2_Sample_Logs.txt sourcetype = SOC Sample Logs


kali-linux-2025.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Search | Splunk
Search | Splunk 10.0.0
localhost:8000/en-US/app/search/search?q=search ip IN ("203.0.113.77"%2C "198.51.100.42")%0A| stats
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Show: 20 Per Page Format Preview: On
user action count
alice malware detected 1
bob connection 1
bob file 3
bob login 1
bob malware detected 1
charlie file 1
charlie login 1
david connection 1
david file 2
david login 3
eve file 1
eve login 1
eve malware detected 1





Note: All sensitive data (IPs, hostnames) in screenshots/reports are synthetic.