



Incident Response Report

Name: Kumari Tulsi

Task 2: Multiple Security Alerts Detected Through Splunk SIEM

Program: Future Interns Cybersecurity Internship

Date: September 2025

Target Application: Splunk SIEM (Analyzed SOC_Task2_Sample_Logs.txt)

Task Summary

This task focused on monitoring and analyzing system logs using Splunk SIEM to identify suspicious activities such as failed logins, unusual IP addresses, and malware detection alerts. The objective was to simulate real-world SOC Analyst responsibilities: threat detection, incident triage, and drafting an incident response report.

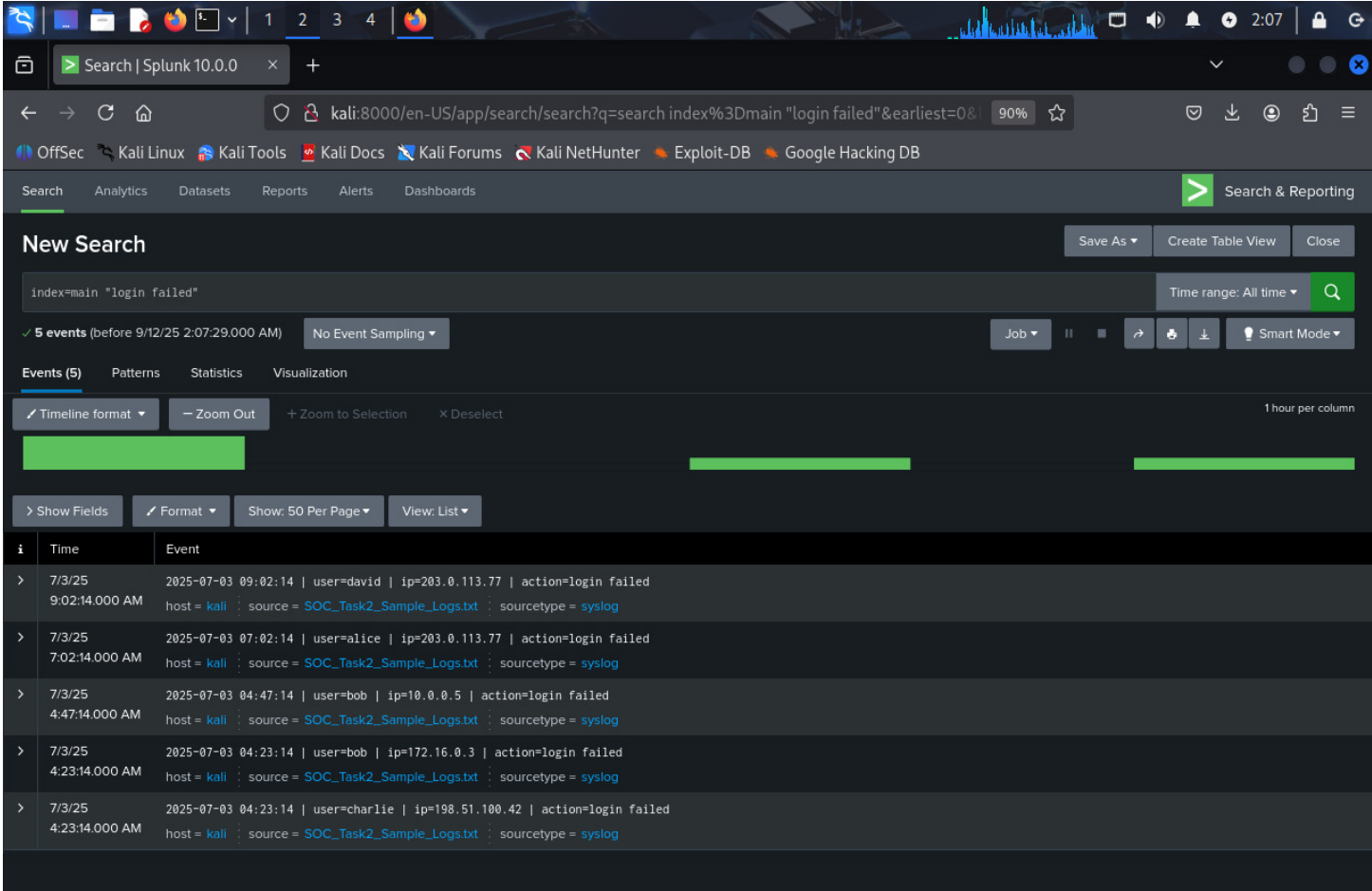
Tools Used

- **Splunk SIEM (Free Trial)** – For log ingestion and analysis
- **Kali Linux** – Host environment
- **SOC_Task2_Sample_Logs.txt** – Sample log dataset provided
- **Manual Analysis & Filtering (grep, Splunk queries)**

Findings

1. Failed Login Attempts

- Multiple failed logins observed from suspicious IPs.
- **Users:** alice, bob, charlie, david
- **IPs:** 203.0.113.77, 10.0.0.5, 198.51.100.42



2. Malware Detection Events

- **Threats:** Ransomware, Rootkit, Trojan, Worm, Spyware
- **Users Involved:** bob, alice, eve, charlie, david
- **IPs Involved:** 172.16.0.3, 198.51.100.42, 192.168.1.101, 203.0.113.77, 10.0.0.5

The screenshot displays the Splunk Search interface. The search bar contains the query `index=main "malware detected"`. The results are shown in a table format with 11 events. Each event entry includes a timestamp, a user name, an IP address, and a threat type. The interface also features a timeline visualization at the top of the results and various controls for filtering and viewing the data.

i	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 = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 user=eve ip=10.0.0.5 action=malware detected threat=Rootkit Signature host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:45:14.000 AM	2025-07-03 07:45:14 user=charlie ip=172.16.0.3 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 user=bob ip=10.0.0.5 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:45:14.000 AM	2025-07-03 05:45:14 user=david ip=172.16.0.3 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:45:14.000 AM	2025-07-03 07:45:14 user=charlie ip=172.16.0.3 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 user=bob ip=10.0.0.5 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:45:14.000 AM	2025-07-03 05:45:14 user=david ip=172.16.0.3 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:30:14.000 AM	2025-07-03 05:30:14 user=eve ip=192.168.1.101 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14 user=bob ip=203.0.113.77 action=malware detected threat=Worm Infection Attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:41:14.000 AM	2025-07-03 04:41:14 user=alice ip=172.16.0.3 action=malware detected threat=Spyware Alert host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:29:14.000 AM	2025-07-03 04:29:14 user=alice ip=192.168.1.101 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:19:14.000 AM	2025-07-03 04:19:14 user=alice ip=198.51.100.42 action=malware detected threat=Rootkit Signature host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog

3. Suspicious External IPs

- IP **203.0.113.77** repeatedly flagged in malware + failed login logs.
- Indicates brute-force or coordinated external attack.

The screenshot shows the Splunk Search interface. The search query is `index=main "203.0.113.77"`. The results show 15 events. The interface includes a timeline view at the top and a table view below. The table view shows the following data:

i	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 = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	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 = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	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 = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	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 = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=203.0.113.77 action=connection attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:18:14.000 AM	2025-07-03 07:18:14 user=bob ip=203.0.113.77 action=file accessed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14 user=alice ip=203.0.113.77 action=login failed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 6:21:14.000 AM	2025-07-03 06:21:14 user=alice ip=203.0.113.77 action=login success host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 6:10:14.000 AM	2025-07-03 06:10:14 user=david ip=203.0.113.77 action=file accessed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=eve ip=203.0.113.77 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:27:14.000 AM	2025-07-03 05:27:14 user=david ip=203.0.113.77 action=connection attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14 user=bob ip=203.0.113.77 action=malware detected threat=Worm Infection Attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:53:14.000 AM	2025-07-03 04:53:14 user=alice ip=203.0.113.77 action=file accessed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:53:14.000 AM	2025-07-03 04:53:14 user=david ip=203.0.113.77 action=login success host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:46:14.000 AM	2025-07-03 04:46:14 user=david ip=203.0.113.77 action=login success host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog

4. User Account Activity (user=bob)

- Logs specifically highlighted suspicious activity tied to **user=bob**.
- Bob's account appears in **ransomware detection** and **failed login attempts**, suggesting it was both **compromised and targeted**.
- **IPs linked to Bob:** 172.16.0.3 (internal system), 203.0.113.77 (external attacker).

The screenshot shows the Splunk Enterprise interface with a search query `index=main "user=bob"` executed. The results are displayed in a table format, showing 14 events. The events are sorted by time, with the most recent at the top. The table columns are Time, Event, and Action. The events show various activities, including login attempts, file access, and malware detection, all associated with the user 'bob'.

i	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 = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:46:14.000 AM	2025-07-03 07:46:14 user=bob ip=10.0.0.5 action=login success host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=192.168.1.101 action=connection attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=203.0.113.77 action=connection attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=192.168.1.101 action=connection attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:44:14.000 AM	2025-07-03 07:44:14 user=bob ip=203.0.113.77 action=connection attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 7:18:14.000 AM	2025-07-03 07:18:14 user=bob ip=203.0.113.77 action=file accessed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 6:01:14.000 AM	2025-07-03 06:01:14 user=bob ip=172.16.0.3 action=file accessed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 user=bob ip=10.0.0.5 action=malware detected threat=Trojan Detected host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:44:14.000 AM	2025-07-03 05:44:14 user=bob ip=198.51.100.42 action=file accessed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14 user=bob ip=203.0.113.77 action=malware detected threat=Worm Infection Attempt host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 5:04:14.000 AM	2025-07-03 05:04:14 user=bob ip=192.168.1.101 action=login success host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:47:14.000 AM	2025-07-03 04:47:14 user=bob ip=10.0.0.5 action=login failed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14 user=bob ip=172.16.0.3 action=login failed host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
>	7/3/25 4:18:14.000 AM	2025-07-03 04:18:14 user=bob ip=198.51.100.42 action=login success host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog

Impact & Risk Assessment

- **Ransomware (bob – 172.16.0.3)** → High risk: Could encrypt data and cause loss.
- **Rootkit (alice – 198.51.100.42, eve – 10.0.0.5)** → High risk: Persistence + privilege escalation.
- **Failed logins (alice, bob, david, charlie)** → Medium risk: Possible brute-force attempts.
- **Suspicious IP 203.0.113.77** → High risk: Multiple attack types from one external source.
- **Compromised User bob** → Critical: Actively targeted + already infected.

Recommendations / Remediation

- Isolate infected systems immediately.
- Block suspicious IPs (esp. 203.0.113.77).
- Reset affected user credentials (Alice, Bob, Eve, Charlie, David).
- Enable MFA and account lockout policies.
- Perform full forensic analysis on compromised hosts.
- Patch and harden internal systems (172.16.0.3, 10.0.0.5, etc.).

Conclusion

Splunk SIEM log monitoring revealed multiple coordinated attacks including malware infections, brute-force login attempts, suspicious external IP activity, and targeted compromise of **user=bob**.

Immediate remediation and strict monitoring actions are required to secure the environment.