INCIDENT RESPONSE REPORT SECURITY OPERATIONS CENTER (SOC) - TASK 2

Date: 30 December 2025
Analyst: MILIND M PATIL
Tools Used: Splunk Enterprise (SIEM)
Severity Level: CRITICAL

1. EXECUTIVE SUMMARY

On July 3, 2025, the SOC team detected a coordinated cyberattack targeting the organization's network. The SIEM (Splunk) alerted on multiple suspicious activities, including brute-force authentication attempts and successful malware infections (Trojans and Ransomware) across several endpoints. The incident has been contained, but immediate remediation is required.

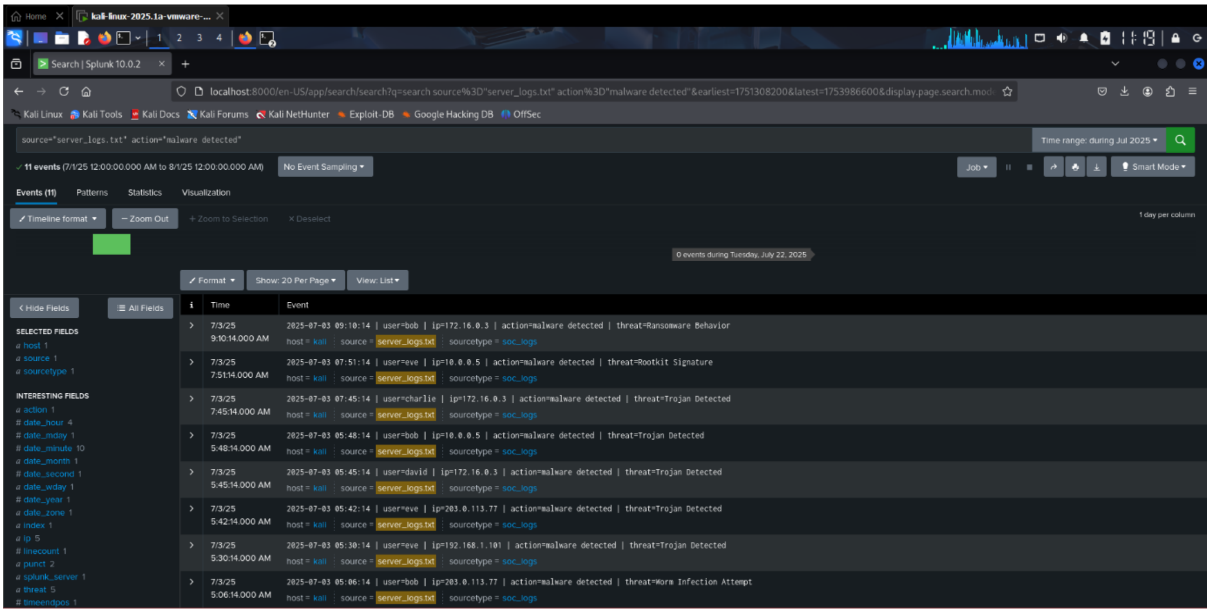
2. INCIDENT TIMELINE

- **04:19 AM:** Initial reconnaissance detected (Connection attempts).
- **04:29 AM:** First malware signature (Trojan) triggered on host 192.168.1.101.
- **05:06 AM:** Worm infection attempt detected on 203.0.113.77.
- **09:10 AM:** Ransomware behavior detected on 172.16.0.3.

3. INVESTIGATION FINDINGS

A. Malware Outbreak (Critical)

- **Description:** Multiple hosts were compromised by malicious software. Splunk logs confirm the presence of Trojans, Rootkits, and Spyware.
- **Affected Hosts:** 10.0.0.5, 172.16.0.3, 192.168.1.101.
- **Evidence:**



```
localhost:8000/en-US/app/search/search?q=search source%3D"server_logs.txt" action%3D"malware detected"&earliest=1751308200&latest=1753986600&display.page.search.mod
```

```
source="server_logs.txt" action="malware detected"
```

✓ 11 events (7/1/25 12:00:00.000 AM to 8/1/25 12:00:00.000 AM)

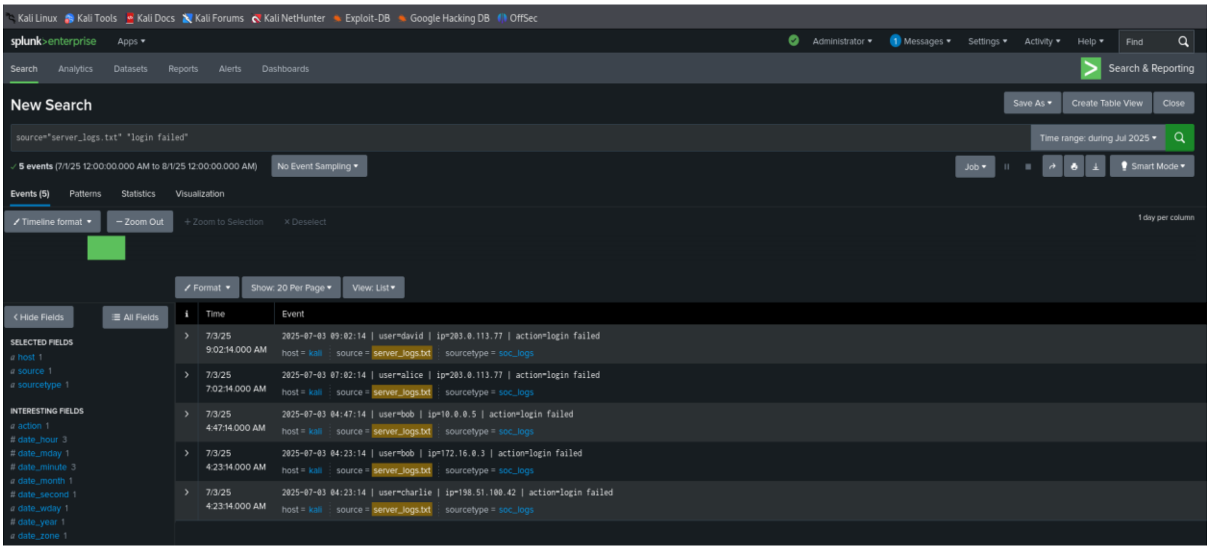
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
# date_hour 4
# date_mday 1
# date_minute 10
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
a date_zone 1
a index 1
a ip 5
# linecount 1
a punct 2
a splunk_server 1
a threat 5
# timeendpos 1

```
i  Time                   Event
>  7/3/25                 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
   9:10:14.000 AM         host = kali   source = server_logs.txt   sourcetype = soc_logs
>  7/3/25                 2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
   7:51:14.000 AM         host = kali   source = server_logs.txt   sourcetype = soc_logs
>  7/3/25                 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
   7:45:14.000 AM         host = kali   source = server_logs.txt   sourcetype = soc_logs
>  7/3/25                 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
   5:48:14.000 AM         host = kali   source = server_logs.txt   sourcetype = soc_logs
>  7/3/25                 2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
   5:45:14.000 AM         host = kali   source = server_logs.txt   sourcetype = soc_logs
>  7/3/25                 2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
   5:42:14.000 AM         host = kali   source = server_logs.txt   sourcetype = soc_logs
>  7/3/25                 2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
   5:30:14.000 AM         host = kali   source = server_logs.txt   sourcetype = soc_logs
>  7/3/25                 2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
   5:06:14.000 AM         host = kali   source = server_logs.txt   sourcetype = soc_logs
```

B. Brute Force Attacks (High)

- **Description:** A high volume of "Login Failed" events was detected, indicating an attempt to guess user passwords.
- **Targeted Users:** David, Alice, Bob.
- **Evidence:**



```
source="server_logs.txt" "login failed"
```

✓ 5 events (7/1/25 12:00:00.000 AM to 8/1/25 12:00:00.000 AM)

i	Time	Event
>	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 = server_logs.txt sourcetype = soc_logs
>	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 = server_logs.txt sourcetype = soc_logs
>	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 = server_logs.txt sourcetype = soc_logs
>	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 = server_logs.txt sourcetype = soc_logs
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed host = kali source = server_logs.txt sourcetype = soc_logs

4. RECOMMENDATIONS & REMEDIATION

1. **Isolate Infected Hosts:** Immediately disconnect 172.16.0.3 and 10.0.0.5 from the network to prevent ransomware spread.
2. **Password Reset:** Force a password reset for users Bob, Eve, and David.
3. **Full Scan:** Run a full antivirus scan on all endpoints.
4. **Firewall Rules:** Block traffic from the external IPs involved in the brute force attempts.