# SOC Task 2 — Incident Response Report

Prepared by: Benny hinn

Date: 10-09-25

Environment: Kali Linux, Splunk

## 1. Executive Summary

During the analysis of the provided log file (Soc\_Task2\_SampleLogs.txt), several suspicious security events were identified. These include multiple malware detections (Trojan, Rootkit, Ransomware, Worm), repeated activity from a suspicious external IP (203.0.113.77), and multiple failed login attempts for certain users. Immediate containment and remediation measures are recommended to prevent potential lateral movement and data compromise.

## 2. Timeline of Key Events

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Timestamp | User | Host/IP | Event Type | Description | Severity |
| 2025-07-03 04:19:14 | alice | 198.51.100.42 | Malware Detected | Rootkit Signature identified | High |
| 2025-07-03 05:06:14 | eve | 10.0.0.6 | Malware Detected | Trojan Detected (multiple times) | High |
| 2025-07-03 05:48:14 | bob | 10.0.0.5 | Malware Detected | Trojan Detected | High |
| Multiple events | — | 203.0.113.77 | External IP Activity | Repeated suspicious connections (15 events) | High |
| 2025-07-03 04:47:14 | bob | 10.0.0.5 | Failed Logins | Multiple login failures, possible brute-force | Medium |

## 3. Impact Assessment

* Affected Users: alice, bob, eve (confirmed malware alerts).
* External Threat Actor: IP 203.0.113.77 repeatedly targeting internal users.
* Possible Risks: Unauthorized access, malware spread, ransomware infection, data theft.

## 4. Containment Actions Taken / Recommended

1. Isolate affected endpoints (10.0.0.5, 10.0.0.6, 198.51.100.42) from the network.  
2. Block external IP 203.0.113.77 at the firewall and IDS/IPS.  
3. Force password resets for users bob, alice, and eve.  
4. Collect forensic artifacts (system logs, memory dumps, disk images) before wiping.  
5. Increase monitoring for repeated failed login attempts across all users.

## 5. Eradication & Recovery Recommendations

1. Reimage infected systems from trusted backups.
2. Run full malware scans with updated signatures.
3. Apply latest OS and application patches.
4. Reconnect systems only after clean verification.
5. Monitor for reinfection or repeat external IP activity for at least 14 days.

## 6. Lessons Learned & Future Prevention

1. Deploy Endpoint Detection & Response (EDR) solutions on all user devices.
2. Enable stricter account lockout policies after repeated login failures.
3. Improve log forwarding from hosts to SIEM (Splunk) for real-time detection.
4. Maintain updated threat intelligence feeds for blocking known malicious IPs.
5. Conduct periodic phishing/malware awareness training for users.

## 7. Appendix

1. Screenshots: Given in Screenshots file
2. SPL Queries Used:  
    index=Internship2 "malware detected" | table \_time user ip threat action  
    index=Internship2 "malware detected" | stats count by user threat | sort -count  
    index=Internship2 action="login failed" | stats count by user ip | sort -count  
    index=Internship2 | stats count by ip | sort -count | head 20