Incident Response Report

Ransomware Attack Detection & Response Using Splunk

1. Executive Summary

A simulated ransomware attack was executed in a controlled environment. The attacker used cron persistence, encrypted files with OpenSSL, and deployed a ransom note. Splunk SIEM detected the behavior in real time, enabling swift containment and full recovery.

2. Lab Architecture

Attacker Machine: Kali Linux, CALDERA, Splunk SIEM
Victim Machine: Ubuntu 22.04, Sandcat Agent, Splunk Forwarder
Log Flow: syslog & auth.log → Forwarder → Splunk SIEM

3. Attack Simulation Overview

• Initial Access (T1059): Remote command execution
• Persistence (T1053): Cron job writing to /tmp/persist.log
• Impact (T1486): File encryption via OpenSSL and ransom note deployment

4. Detection & Alerting (Splunk SIEM)

• Suspicious Root Cron Persistence – T1053
• Ransomware Encryption Activity – T1486

5. Incident Investigation

IOCs:
- /etc/cron.d/persist_test
- /tmp/persist.log
- .locked encrypted files
- README_RESTORE.txt

6. Containment & Eradication

• Removed malicious cron entry
• Deleted persistence file
• Terminated malicious processes

7. Recovery

Executed decryption script, restored all encrypted files, and validated system integrity.

8. MITRE Mapping

T1059 – Command Execution
T1053 – Cron Persistence
T1486 – Data Encrypted for Impact

9. Lessons Learned

- Cron persistence requires behavioral detection
- File encryption logs are often minimal
- SIEM correlation and EDR tools enhance detection

10. Conclusion

The project demonstrates realistic SOC incident handling—from attack detection to containment and full recovery.