The monitoring component for ransomware detection was implemented using OSSEC HIDS (Host Intrusion Detection System). The tool operates at the host level, analyzing system logs, tracking file changes, and generating alerts whenever suspicious activity is detected.

OSSEC was installed locally on a Kali VM using the source-based setup method (with *local* mode selected since we are using the rubber ducky attack method). After installation, its configuration file /var/ossec/etc/ossec.conf was modified to monitor target system directories and logs. The main directory under observation was /home/kali/Desktop/personal\_Fa0337, which was designated as the target folder for simulated ransomware encryption. Additional system logs such as /var/log/syslog and /var/log/auth.log were included to detect any anomalous system-level or authentication-related events.

Custom detection rules were created in the local\_rules.xml configuration file. These rules were designed to raise alerts for patterns indicative of ransomware behavior including multiple file write operations, encryption signatures, or sudden file renaming events. The system analyzed logs and file checksums, triggering alerts when modifications deviated from the expected values.

All monitoring data was recorded in structured log files located in /var/ossec/logs/alerts/alerts.log and /var/ossec/logs/ossec.log. These logs contain data such as timestamps, rule IDs, file paths, and alert levels, allowing for detailed analysis for detection.

To save the data onto MySQL Database server, we wrote a small python script which parsed /var/ossec/logs/alerts/alerts.log and added them to respective columns in the ossec\_alerts table.

Please find below alerts.log when rubber ducky attack occurs:





