Group:	Report Number:	Report id
Essential Group	Report No. 6	6-4-essential-cyber-scenario-soc&hids

Syscheck Configuration

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Date of Task Assignment :

1/17/2026

Due Date:
1/20/2026

Contents

Scenario:

•Task: Navigate to the configuration directory and set up a 10-hour frequency for system integrity scans.

•Step: Edit /var/ossec/etc/ossec.conf.

Question: Which section of the ossec.conf file is responsible for defining which directories to monitor for file integrity?

Assessing the OSSEC file comigration

access the OSSEC configuration file as administrator in the following directory:

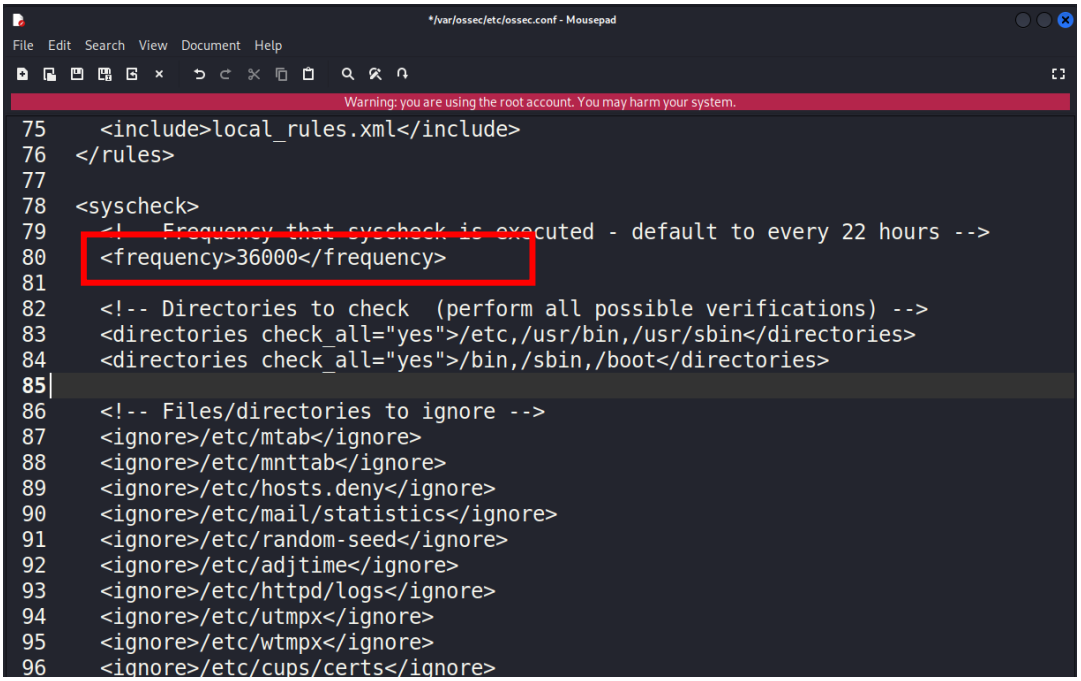
/var/ossec/etc/ossec.conf

We used mousepad here for more visual ui

Set the time frequency

The Scan Frequency Set the integrity scan frequency to **10 hours**. Since OSSEC uses seconds for scheduling:

- **10 hours = 10 × 60 × 60 =** 36,000 seconds



File Integrity Monitoring Configuration

The Syscheck engine is the OSSEC component specifically designed to perform File Integrity Monitoring (FIM). Within the ossec.conf file, all FIM-related settings, including scan frequency and directory definitions, are configured inside the <syscheck> section.

This section determines:

- Which directories and files are monitored
- How often integrity scans occur
- What attributes are checked (permissions, ownership, checksums, and file size)

The Syscheck engine plays a vital role in maintaining system security by detecting unauthorized file changes. By correctly configuring the <syscheck> section in ossec.conf, administrators can establish an effective integrity baseline and ensure regular monitoring of critical system directories. Setting an appropriate scan frequency, such as 10 hours, balances security monitoring with system performance.