

**Group:**  
Essential Group

**Report Number:**  
Report No. 6

**Report id**  
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

<b>Assessing the OSSEC file comigration .....</b>	<b>2</b>
<b>Set the time frequency.....</b>	<b>2</b>
<b>File Integrity Monitoring Configuration .....</b>	<b>3</b>

## 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`.

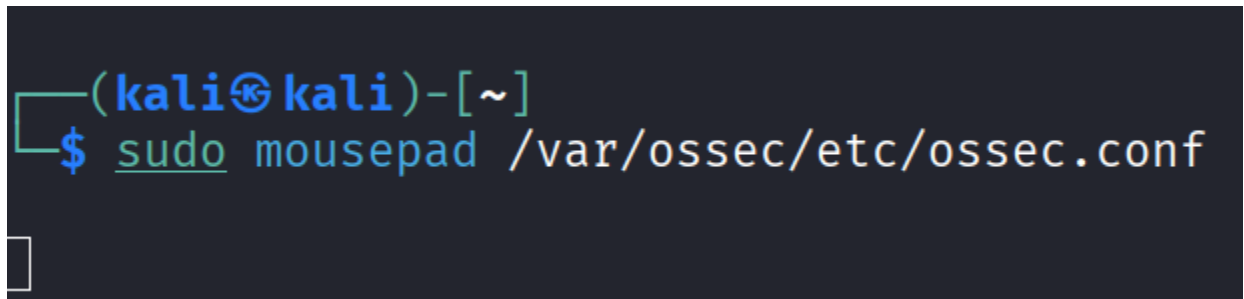
**Question:** Which section of the `ossec.conf` file is responsible for defining which directories to monitor for file integrity?

---

## Assessing the OSSEC file configuration

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

`/var/ossec/etc/ossec.conf`



```
(kali@kali)-[~]
└─$ sudo mousepad /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** =  $10 \times 60 \times 60 = 36,000$  seconds

```
*var/ossec/etc/ossec.conf - Mousepad
Warning: you are using the root account. You may harm your system.
75 <include>local_rules.xml</include>
76 </rules>
77
78 <syscheck>
79 <!-- Frequency that syscheck is executed - default to every 22 hours -->
80 <frequency>36000</frequency>
81
82 <!-- Directories to check (perform all possible verifications) -->
83 <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
84 <directories check_all="yes">/bin,/sbin,/boot</directories>
85|
86 <!-- Files/directories to ignore -->
87 <ignore>/etc/mtab</ignore>
88 <ignore>/etc/mnttab</ignore>
89 <ignore>/etc/hosts.deny</ignore>
90 <ignore>/etc/mail/statistics</ignore>
91 <ignore>/etc/random-seed</ignore>
92 <ignore>/etc/adjtime</ignore>
93 <ignore>/etc/httpd/logs</ignore>
94 <ignore>/etc/utmpx</ignore>
95 <ignore>/etc/wtmpx</ignore>
96 <ignore>/etc/cups/certs</ignore>
```

## 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.