¿Qué es OSSEC?

OSSEC es un sistema de detección de intrusos basado en host (HIDS) de código abierto y gratuito. Realiza análisis de registros, verificación de integridad, detección de rootkit, alertas basadas en el tiempo y respuesta activa. (Wikipedia)

Consta de dos componentes principales

- El **servidor**: se encarga de monitorear y registrar la actividad de los agentes
- **Agentes**: se instalan en cada una de las máquinas que se quiere supervisar y envía la información que recoge al servidor. Pueden ser Windows, Linux y Mac

Tiene una versión de pago llamada ATOMIC ENTERPRISE OSSEC

Se puede descargar de los repositorios, desde su web o desde github: https://github.com/ossec

HIDS - OSSEC

Se instala en /var/ossec/ y su fichero de configuración es /var/ossec/etc/ossec.conf.

Función de sus directorios

- /**bin** – Todos los ficheros ejecutables.
- /**etc** – Ficheros de configuración
- /**logs** – Ficheros de log donde registrará las alertas. El principal es alerts/alerts.log
- /**queue** – Ficheros de colas de proceso.
- /**rules** – Ficheros que contienen las reglas que generan las alertas.
- /**stats** – Estadísticas
- /**tmp** – Directorio temporal
- /**var** – Contiene un fichero con el PID de cada proceso de OSSEC

HIDS - OSSEC

Ejecutables principales

- **ossec-control** : Administra os demonios de OSSEC. Inicia, para, reinicia, etc.
- **agent_control**: Permite consultar y obtener información de cualquier agente. También le permite reiniciar (ejecutar ahora) el escaneo syscheck / rootcheck en cualquier agente.
- **manage_agents**: Gestiona las claves de autenticación para agentes. Estas claves de autenticación son necesarias para la comunicación segura (encriptada y autenticada) entre el servidor OSSEC y sus instancias de agentes.
- **syscheck_control**: Administra la base de datos de verificación de integridad.
- **rootcheck_control**: Administra la base de datos de supervisión de políticas y auditoría del sistema que se almacena en el lado del servidor. Puede enumerar las anomalías detectadas por la función rootcheck, clasificadas en problemas resueltos y pendientes. Además, puede averiguar cuándo se ejecutó ossec-rootcheck por última vez.