1.INTRODUCCIÓN

El objeto de este proyecto es la creación de una plataforma de correlación de eventos de seguridad.

En la actualidad podemos disponer de multitud de máquinas y software para la gestión de seguridad, monitorización, administración de redes etc. A cada módulo software que sea capaz de emitir un tipo de mensaje al detectar un evento lo llamaremos sensor.

Una red compleja puede tener sensores de IDS ([1]), de cortafuegos, de autenticación, de control del QoS ([2]) etc, los cuales, correctamente configurados, pueden emitir logs (o almacenarlos en un fichero) del tipo "Detección de escaneo de puertos", "Error de autenticación como administrador", "Ocupación del ancho de banda por encima del 90% asignado", "Intento de intrusión desde 207.137.23.152" etc.

Ante este escenario heterogéneo tanto de hardware, sistema operativo, software y sintaxis de los mensajes que emiten los sensores, los problemas fundamentales que resuelve esta plataforma de correlación de eventos de seguridad son los siguientes:

- Normalización del formato de los mensajes de los distintos sensores.
- Almacenamiento de los mensajes normalizados en una base de datos.
- Consulta, modificación y clasificación de los mensajes.
- Generación de estadísticas y filtrado de datos.
- Generación de informes detallados.

Los mensajes de los distintos sensores se normalizarán de acuerdo al *draft* **IDMEF**. El software elegido para el almacenamiento de los mensajes IDMEF en la base de datos ha sido **Prelude**, tras el estudio comparativo estudiarlo junto con Foresight. Las operaciones citadas en los tres últimos puntos se ha realizado desarrollando la librería Marte Alert en java.

1.1.Fases del proyecto.

- Documentación sobre estándares para la normalización: IDMEF.
- Estudio de Prelude-IDS.
- Estudio de Foresight.
- Instalación y configuración de Prelude-IDS y Prewikka.
- Estudio de PostgreSQL
- Estudio de clases java gráficas.
- Desarrollo de la librería java Marte Alert.
- Optimización temporal de las peticiones SQL.
- Desarrollo del diálogo gráfico para filtrado.
- Configuración de reglas del Snort-IDS.
- Fase de testeo y corrección de fallos (bugs).

[1] Sistema de detección de intrusiones (Intrusion Detection System)

[2] Gestión del ancho de banda o calidad del servicio (Quality of Service)