RESUMEN

En este proyecto de titulación se busca analizar una herramienta para realizar la gestión, monitoreo y registro de eventos de seguridad de informática, desarrollando un prototipo de gestor basado en herramientas de software libre, que se ajuste a cualquier modelo de red a través de un fácil despliegue y bajo costo. Dentro de la gestión se busca mejorar la disponibilidad y el marco entorno a la seguridad de la red, la monitorización se la realiza mediante mecanismos que permiten verificar el estado de los equipos que conforman la red, además de generar un registro ordenado de eventos que en su medida pueden dañar o no la disponibilidad y autenticidad de la información. El propósito de este trabajo es diseñar un prototipo portable (máquina virtual) basado en la plataforma de código abierto OSSIM, misma que permite una gestión centralizada e intuitiva, que facilita la detección de eventos y vulnerabilidades en la red. Se detalla la arquitectura, configuración y análisis de los resultados obtenidos con la herramienta, tomado en cuenta la aplicación de directrices de seguridad establecidos por entidades de normalización internacionales ISO/INEN.

PALABRAS CLAVES

- **GESTIÓN DE RED**
- **SEGURIDAD DE LA INFORMACIÓN**
- **DETECCIÓN DE EVENTOS**
- **DETECCIÓN DE VULNERABILIDADES**
- **POLÍTÍCAS DE SEGURIDAD**

ABSTRACT

This project aims to analyze a tool to perform the management, monitoring and registration of computer security events, developing a prototype manager based on free software tools, which will fit any network model through an easy Deployment and low cost. Within the management it is sought to improve the availability and the framework around the network security, the monitoring is done through mechanisms that allow to verify the state of the equipment that make up the network, in addition to generating an ordered register of events that in Their measurement may or may not damage the availability and authenticity of the information. The purpose of this paper is to design a portable prototype (virtual machine) based on the open source OSSIM platform, which allows a centralized and intuitive management that facilitates the detection of events and vulnerabilities in the network. It details the architecture, configuration and analysis of the results obtained with the tool, taking into account the application of safety guidelines established by ISO / INEN international standardization entities.

KEYWORDS

- **NETWORK MANAGEMENT**
- **INFORMATION SECURITY**
- **EVENT DETECTION**
- **VULNERABILITY DETECTION**
- **SECURITY POLICIES**