Sensor para recopilación y visualización de información de seguridad en nodos de una red

Moisés Gautier Gómez

Palabras clave

Iptables, Seguridad informática, Paquetes, Eventos, Python, Sonda, Django, Web, Visualización

Resumen

El objetivo principal del proyecto es desarrollar un software que permita recopilar y visualizar la información generada por las aplicaciones de monitorización y control de seguridad que se ejecutan en una máquina.

La motivación del mismo surge fruto de la necesidad de monitorizar un red corporativa a través de un mecanismo de gestión automatizada de eventos (SIEM). Los pasos para la realización de este sistema se han modularizado y dividido en diferentes etapas que se desarrollarán como un todo dentro del proyecto de investigación VERITAS (http://nesg.ugr.es/veritas/) del Network Engineering & Security Group (NESG - http://nesg.ugr.es/) perteneciente al área de Ingeniería Telemática de la Universidad de Granada.

Para esta finalidad será necesario definir los pasos para la obtención de logs de una fuente de seguridad, configurar la instalación para dicha fuente, realizar un sistema de parseo de logs para extraer la información, almacenarla en un sistema persistente (base de datos) y visualizarla mediante una interfaz web en la sonda desplegada.

Por último, para comprobar la efectividad y analizar el funcionamiento de la solución software, se realizaría una demostración en directo con procesamiento real de eventos para la fuente de seguridad cuyo ámbito tiene este proyecto, que será Iptables.