Sensor for collecting and displaying information security network nodes

Moisés Gautier Gómez

Keywords

Iptables, Computer security, Packets, Events, Python, Probe, Django, Web, Visualization

Abstract

The main objective of the project is to develop a software to collect and display information generated by monitoring applications and security controls running on a machine.

The motivation arises because of the need to monitor a corporate network through a mechanism of automated event management (SIEM). The steps for the implementation of this system are modularized and divided into different stages to be developed as a whole within the research project VERITAS (http://nesg.ugr.es/veritas/) of the Network Engineering & Security Group (NESG - http://nesg.ugr.es/), that belogs to the area of Telematic Engineering of the University of Granada.

For this purpose it is necessary to define the steps to obtain logs of a security source, configure the installation for that source, perform system parsing logs to extract the information, store the data in a persistent system (database) and visualize these data via a web interface.

Finally, to test the efectiveness and analyze the performance of the software solution, a demonstration is done with actual live events processing from Iptables.