Sensor for collecting and displaying information security network nodes

Moisés Gautier Gómez

Keywords

Iptables, Informatic 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 control 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 realization 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/) fo Network Engineering & Security Group (NESG - http://nesg.ugr.es/) belonging 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, stored in a persistent system (database) and view via a web interface on the probe deployed.

Finally, to test the efectiveness and analyze the performance of the software solution, a demonstration would be done with actual live event processing for security source project whose scope has to be Iptables.