Alert correlation framework using a novel clustering approach

Abstract

Currently, the primary and pressing issue in IDS implementation is the enormous number of alerts generated by the IDS sensors. Moreover, due to this obtrusive predicament, two other problems have emerged, first is the difficulty in processing the alerts accurately and second is the reduction in performance rate in terms of time and memory capacity while processing these alerts. The purpose of this research is to construct a holistic solution that is able to firstly reduce the number of alerts to be processed and at the same time produce a high quality attack scenarios that are meaningful to the administrators in a timely manner. To achieve these goals, alerts generated by IDS sensors need to be correlated and organized in an appropriate approach. Thus the significant contribution of this research is to create an integrated operational framework for alert processing that reduces the amount of alerts to be processed and creates more meaningful attack scenarios to be analyzed. We are presenting the results obtained from the clustering algorithm and discuss its significant contribution to practitioners in an actual working environment.