Abstract

Intrusion Detection System (IDS) is a well known security feature and widely implemented among practitioners. However, since the creation of IDS the enormous number of alerts generated by the detection sensors has always been a setback in the implementation environment. Moreover due to this obtrusive predicament, two other problems have emerged which are the difficulty in processing the alerts accurately and also the decrease in performance rate in terms of time and memory capacity while processing these alerts. Thus, based on the specified problems, the purpose of our overall research is to construct a holistic solution that is able to reduce the number of alerts to be processed and at the same time to produce a high quality attack scenarios that are meaningful to the administrators in a timely manner. In this paper we will present our proposed framework together with the result of our novel clustering method, architected solely with the intention of reducing the amount of alerts generated by IDS. The clustering method was tested against two dataset; a globally used dataset, DARPA and a live dataset from a cyber attack monitoring unit that uses SNORT engine to capture the alerts. The result obtained from the experiment is very promising; the clustering algorithm was able to reduce about 86.9% of the alerts used in the experiment. From the result we are able
An Operational Framework for Alert Correlation using a Novel Clustering Approach

to highlight the contribution to practitioners in an actual working environment.

References

Recent Advances in Intrusion Detection (RAID 2000), Toulouse, France.

Index Terms
Computer Science
Security

Keywords
IDS clustering hashing technique