Abstract

Numerous techniques and approaches are used to address the threats that are faced by computer networks today's. Some of these reactive approaches involve Intrusion Detection System (IDS), malware data mining and network monitoring. Numerous false positive alerts are generated by the IDS, contributing negatively to system complexity and performance. In this paper, we present a new framework called collection mechanism and reduction of IDS alert framework (CMRAF) to remove duplicate IDS alerts and reduce the amount of false alerts. CMRAF is based on two models. The first model develops a mechanism to save IDS alerts, extract the standard features as intrusion detection message exchange format, and save them
in DB file (CSV-type). The second model consists of three phases. The first phase removes redundant alerts, the second phase reduces false alerts based on threshold time value, and the last phase reduces false alerts based on rules with threshold common vulnerabilities and exposure value. We applied CMRAF on two environments: the Darpa 1999 and the NAv6 network center data sets. The result obtained from the experiment on Darpa 1999 data set recorded an 92% alert reduction rate, whereas that on the NAv6 data set recorded an 84% alert reduction rate. From the results, CMRAF was able to scale back a massive quantity of redundant alerts and effectively reduces false alerts.

References

- Common-Vulnerabilities-and-Exposures

**Index Terms**

Computer Science

Security
Keywords
False positive  Reduction alert  Network security  IDS  Aggregation alert