Design of a Hybrid Intrusion Detection System using Snort and Hadoop

Abstract

Security is the most important issue that is to be considered in any environment. Any attack can be launched from any node. Any of these attacks should be identified and subsequent actions should be taken to avoid further consequences. An intrusion detection system helps in identifying the attacks at the early stage and give alarms. These intrusion detection systems should be able to identify almost any kind of attacks, be it a newly launched one or a pre-established one. In this work, the intrusion detection system Snort is made use of. In this work, the packets captured by Snort is analyzed by the Grid computing framework Hadoop, which is used for Big Data Analysis. For more user friendly analysis a data warehouse system for Hadoop, Hive is also provided. For those ip addresses that generate large number of packets, Snort rules will be generated so that when the number of packets from a particular source exceeds a number, the node will generate alerts to other nodes since there is a possibility of attack.

References

- W. Chen, W. Kuo and Y. Wang, Building IDS Log Analysis System on Novel Grid
Design of a Hybrid Intrusion Detection System using Snort and Hadoop

Computing Architecture, National Center for High-Performance Computing, Taiwan, 2009
- B. E. Lavender, Implementation of Genetic Algorithm into a Network Intrusion Detection System (netGA) and Integrating to nProbe, Thesis Work
- T. White and P. W. Daly, Hadoop-The Definitive Guide, O'Reilly

Index Terms
Computer Science
Security

Keywords
Hadoop  Hive  MapReduce  Snort  Rules