Abstract

Network Intrusion Detection Systems (NIDSs) are systems that monitor computer networks to detect, identify and prevent the malicious events, which attempt to compromise the integrity, confidentiality or availability of computer networks. The NIDS may be classified according to the detection technique into two types, the "Signature-Based" and "Anomaly-Based" NIDS. In order to increase the efficiency of the NIDS, a hybrid signature-anomaly NIDS based on both snort and negative selection algorithm is proposed. To evaluate the efficacy of the proposed system the 1999 DARPA data set is used. The experimental results show that the performance of the proposed system is more efficient than using snort on its own.

References


23. Thomas, C., V. Sharma, and N. Balakrishnan, Usefulness of DARPA dataset for intrusion detection system evaluation, in Data Mining, Intrusion Detection, Information Assurance and Data Networks Security. 2008.

Index Terms

Computer Science

Networks

Keywords

Signature Based, Anomaly Based, Snort, Negative Selection