Abstract

With the rapidly growing and wide spread use of computer networks the number of new threats has grown extensively. Intrusion and detection system can only identifying and protecting the attacks successfully. In this paper we focus on detailed study of different types of attacks using in KDD99CUP Data Set and classification of IDS are also presented. They are Anomaly Detection System, Misuse Detection Systems. Different Data Analysis Methodologies also explained for IDS. To identify eleven data computing techniques associated with IDS are divided groups into categories. Some of those methods are based on computation such as Fuzzy logic and Bayesian networks, some are Artificial Intelligence such as Expert Systems, agents and neural networks some other are biological concepts such as Genetics and Immune systems.

Reference
Intrusion Detection System Methodologies Based on Data Analysis

- Theodoros Lapps and Konstantinos Pelechrinis “Data Mining Techniques for (Network) Intrusion Detection Systems” Department of Computer Science and Engineering UC Riverside, Riverside CA 92521.
Intrusion Detection System Methodologies Based on Data Analysis


Index Terms

Computer Science Security

Key words

IDS

KDD Data Set

Anomaly Detection System

Misuse Detection

Data computing Techniques