Abstract

Intrusion detection system (IDS) is a kind of security management model that can be installed in computers and networks. IDS gather information from the network and computer and analyses it to find the possible security breaches into the system, which contain both intrusions and misuse. If we see modern IDS they also have few vulnerabilities, these systems also have drawbacks of false detection. So we aim to make a new model which can decrease the possibilities of false detection. In this paper we have done a survey of different algorithm used in intrusion detection system and then designed a new model that will use correlation based feature selection algorithm and SVM. This model will be tested on KDDCup99 dataset.

References


3. Jeffrey Erman, Martin Arlitt, Anirban Mahanti, “Traffic Classification Using Clustering Algorithms”, University of Calgary, 2500 University Drive NW, Calgary, AB, Canada

4. MR Shanmugavadivu, “KDD Cup 99 Dataset” 2015


11. Building Efficient Intrusion Detection Model Based on Principal Component Analysis and C4.5 You Chen', Yang Li, Xue-Qi Cheng1, Li Guo


13. Mr. Vijay D. Katkar, Mr. Siddhant Vijay Kulkarni, “Experiments on Detection of Denial of Service Attacks using Naive Bayesian Classifier” 2013


Index Terms

Computer Science Security

Keywords
NIDS, HIDS, KDDCUP9 DATASET, CFS, SVM, U2R, R2L, PROBE, DoS