Abstract

In this paper, intrusion detection is to detect attacks (Intrusions) against a computer system. In the highly networked modern world, conventional techniques of network security such as cryptography, user authentication and intrusion prevention techniques like firewalls are not sufficient to detect new attacks. In this paper, we perform experiments on the kddcup99 data set. We perform dimensionality reduction of the data set using PCA (principal Component Analysis) and clear distinction between normal and anomalous data is observed by using supervised data mining techniques. Primarily experiments with kddcup99 network data show that the supervised techniques such as Naïve Bayesian, C4.5 can effectively detect anomalous attacks and achieve a low false positive rate. In this thesis optimization technique such as Random Forest has applied to improve the efficiency of detection rate and achieve a low false positive rate. This mechanism can effectively tolerate intrusion.

References

Intelligence, 2009.
- Michael D. Alder &quot;An Introduction to Pattern Recognition: Statistical, Neural Net and Synthetic Methods of getting robots to see and hear;&quot; September19,1997http://ciips.ee.uwa.edu.au/mike/PatRec
- White, Mark ECE591Q-Machine Learning – Lecture slides, Fall 2005
- Prabhjeet Kaur , Amit Kumar Sharma, Sudesh Kumar Prajapat "MADAM ID FOR INTRUSION DETECTION USING DATA MINING" IJRIM Volume 2, Issue 2 (February
2012) (ISSN 2231-4334).

Index Terms

Computer Science
Security

Keywords
Data Mining
Naive Bayes Classifier
classification Tree
Anomaly Detection
Systems (ADS)
kddcup99
PCA