Abstract

Data mining refers to extracting knowledge from large amounts of data. Most of the current
systems are weak at detecting attacks without generating false alarms. Intrusion detection systems (IDSs) are increasingly a key part of system defense. An intrusion can be defined as any set of actions that compromise the integrity, confidentiality or availability of a network resource (such as user accounts, file system, kernels & so on). Data mining plays a prominent role in data analysis. In this paper, classification techniques are used to predict the severity of attacks over the network. I have compared zero R classifier, Decision table classifier & Random Forest classifier with KDDCUP 99 databases from MIT Lincoln Laboratory.

References

- Macros.M. Campos, Boriana L. Milenora, “ Creation & Deployment of Data Mining based
A Comprehensive Analysis and study in Intrusion Detection System using Data Mining Techniques


Index Terms

Computer Science
Security
Keywords

Data Mining      Intrusion Detection      Machine Learning
                 Zero R

Decision Table & Random Forest classifier

KDDCup99 dataset