World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:06, 2014

Detecting Venomous Files in IDS Using an Approach Based on Data Mining Algorithm

Authors : Sukhleen Kaur

Abstract : In security groundwork, Intrusion Detection System (IDS) has become an important component. The IDS has received increasing attention in recent years. IDS is one of the effective way to detect different kinds of attacks and malicious codes in a network and help us to secure the network. Data mining techniques can be implemented to IDS, which analyses the large amount of data and gives better results. Data mining can contribute to improving intrusion detection by adding a level of focus to anomaly detection. So far the study has been carried out on finding the attacks but this paper detects the malicious files. Some intruders do not attack directly, but they hide some harmful code inside the files or may corrupt those file and attack the system. These files are detected according to some defined parameters which will form two lists of files as normal files and harmful files. After that data mining will be performed. In this paper a hybrid classifier has been used via Naive Bayes and Ripper classification methods. The results show how the uploaded file in the database will be tested against the parameters and then it is characterised as either normal or harmful file and after that the mining is performed. Moreover, when a user tries to mine on harmful file it will generate an exception that mining cannot be made on corrupted or harmful files.

Keywords : data mining, association, classification, clustering, decision tree, intrusion detection system, misuse detection, anomaly detection, naive Bayes, ripper
Conference Title : ICADMA 2014 : International Conference on Advanced Data Mining and Applications
Conference Location : Istanbul, Türkiye
Conference Dates : June 19-20, 2014