Abstract

Security is a big issue for all networks in today’s enterprise environment. Hackers and intruders have made many successful attempts to bring down high profile company networks and web services. Intrusion Detection System (IDS) is an important detection that is used as a countermeasure to preserve data integrity and system availability from attacks. The main
Intrusion Detection through Ensemble Classification Approach

Reason for using data mining classification methods for Intrusion Detection System is due to the enormous volume of existing and newly appearing network data that require processing. Data mining is the best option for handling such type of data. This paper presents the new idea of applying data mining classification techniques to intrusion detection systems to maximize the effectiveness in identifying attacks, thereby helping the users to construct more secure information systems. This paper uses ensemble approach with K nearest neighbors and Decision trees for intrusion detection. The ensemble method is advantageous over single classifier. In this novel class can be detected for attack is reported to user in case of attack detection. An Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. An Intrusion Detection System has a database of attack signatures. The attack signatures are patterns of different types of previously detected attacks. In case it finds a match, the system reports the malicious activity to the management console.

Reference

- Hongbo Zhu, Yaqiang Wang, Zhonghua Yu “Clustering of Evolving Data Stream with Multiple Adaptive Sliding Window” 2010 International Conference on Data Storage and Data Engineering.
- Peng Zhang, Xingquan Zhu, Jianlong Tan, Li Guo “Classifier and Cluster Ensembles for Mining Concept Drifting Data Streams” 2010 IEEE International Conference on Data Mining
- Yongjin Liu , NaLi, Leina Shi, Fangping Li “An Intrusion Detection Method Based on Decision Tree” 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies
- LID Li-xiong, KANGJing, GUO Yun-fei, HUANGHai “A Three-Step Clustering Algorithm over an Evolving Data Stream” The National High Technology Research and Development Program(“863” Program) of China, Fund 2008 AA01002 sponsors.
- Mrutyunjaya Panda, Manas Ranjan Patra “A COMPARATIVE STUDY OF DATA MINING ALGORITHMS FOR NETWORK INTRUSION DETECTION” 2008 First International Conference on Emerging Trends in Engineering and Technology
- Shuang Wu, Chunyu Yang and Jie Zhou “Clustering-training for Data Stream Mining” Sixth IEEE International Conference on Data Mining - Workshops (ICDMW’06)

Index Terms

Computer Science

Data Mining

Key words

Data mining

ensemble approach

K-nearest neighbors

K-means algorithm

Decision Trees

security

IDS