Abstract

Network intrusion detection system includes identifying a set of spiteful actions that compromises the basic security requirements such as integrity, confidentiality, and availability of information resources. The enormous increase in network attacks has made the data mining based intrusion detection techniques extremely useful in detecting the attacks. This paper
Network Intrusion Detection using Clustering: A Data Mining Approach
describes a system that is able to detect the network intrusion using clustering concept. This
unsupervised clustering technique for intrusion detection is used to group behaviors together
depending on their similarity and to detect the different behaviors which are then grouped as
outliers. Obviously, these outliers are attacks or intrusion attempts. This proposed method
which uses data mining technique will reduce the false alarm rate and improves the security.

Reference

- Buyer's guide for intrusion prevention systems (IPS), June 3, 2004
  (http://www.juniper.net/solutions/literatur/buryerguide/ 710005.pdf)
- Dunigan and Hinkel, Intrusion detection and intrusion prevention on a large network, a
  case study," in Proceedings of the 1st Workshop on Intrusion Detection and Network
  Monitoring, Apr. 1999.
- Goverdhan Singh, Florent Masseglia, et al Data Mining for Intrusion Detection: from
  Outliers to True Intrusions, published in "The 13th Pacific-Asia conference on Knowledge
  Discovery and Data Mining (PAKDD-09) (2009) 891-898"
- J. Han and M.Kamber, Data Mining: Concepts and Techniques, Morgan Kaufmann
- B. Hay, G. Wets and K. Vanhoof, “Clustering Navigation Patterns on a Website using a
- Kazimierz Kowalski and Mohsen Beheshti Improving Security Through Analysis of Log
- W. Lee, S. J. Stolfo, and P. K. Chan, Real Time Data Mining-based Intrusion Detection,” in
  (http://citeseer.ist.psu.edu/452795.html)
- W. Lee and S. J. Stolfo. Data mining approaches for intrusion detection. In 7th
  In The 13th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD’09),
  Method for Sequences of Categorical Values”, Proc.5th Pacific-Asia Conf. Knowledge Mining,
  Kowloon, HongKong 2001.
- Seung-Joon Oh, Jae-Yeamin Kim, “Clustering Categorical Sequences Using a
  No.3,141-150,Sept 2005.
- A. Valdes and K. Skinner. Probabilistic alert correlation In Recent Advances in Intrusion
Index Terms

Computer Science
Network Security

Key words

Intrusion Detection
Security
Clustering

Classification

Common Outliers