Abstract

Intrusion detection plays vital role in computer network security since long. Experience has shown that most IDS struggle for curbing false positive rate. As part of our proposed model with the objective of reducing false positive rate here we have focused on preprocessing functionality. The main objective of our preprocessing module is to reduce ambiguity and provide accurate information to detection engine. So here we have presented preprocessing module which cleans network data and handles missing or incomplete data. Preprocessing module is highly configurable. Based on the result of vulnerability assessment and network topology, hosts exists, services running, intrusion detection analyst need to configure preprocessing module. Effectiveness of preprocessing module depends on such configuration parameters and in turn knowledge of intrusion detection analyst. Preliminary analysis of our approach has shown reduction in false positive rate.

References


- Ashley Thomas, RAPID: Reputation based approach for improving intrusion detection effectiveness, Sixth International Conference on Information Assurance and Security (IAS), Atlanta, GA, 2010


- Brian Eugene Lavender, Implementation of Genetic Algorithms into a Network Intrusion Detection System (netGA), and Integration into nProbe, M. S. Project, CALIFORNIA STATE UNIVERSITY, SACRAMENTO, 2010


- Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, Shaidah Jusoh, Distributed and
Cooperative Hierarchical Intrusion Detection on MANETs, International Journal of Computer Applications (0975 – 8887) Volume 12– No. 5, December 2010
- Kai Hwang, Min Cai, Ying Chen, Min Qin, Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 4, NO. 1, JANUARY-MARCH 2007
- Obbo Aggrey, An Intrusion Detection System For Academic Institutions, Master of Science Thesis, Makerere University, July 2007
Data Preprocessing for Reducing False Positive Rate in Intrusion Detection

- Salem Benferhat, Karima Sedki, Karim Tabia, PREPROCESSING ROUGH NETWORK TRAFFIC FOR INTRUSION DETECTION PURPOSES, IADIS International Telecommunications, Networks and Systems 2007
- Sung-Bae Cho and Sang-Jun Han, Two Sophisticated Techniques to Improve HMM-Based Intrusion Detection Systems, Lecture Notes in Computer Science, Volume 2820/2003, SpringerLink, 2003

Index Terms

Computer Science  
Network Security
Keywords
Preprocessing  Intrusion Detection  false positive reduction