عنوان مقاله:
(Anomaly-based intrusion detection system using Relational Detector Tree (RTD

محل انتشار:
دومین کنفرانس بین المللی مهندسی برق و علوم کامپیوتر (سال: 1394)

تعداد صفحات اصل مقاله: 8

نویسندگان:

Mohammad Dabiri - *Department of Computer, Buinzahra Branch, Islamic Azad University, Buinzahra, Iran*

Khashayar Khosharay - *Department of Computer, Buinzahra Branch, Islamic Azad University, Buinzahra, Iran*

Golnoush Abaei - *Shahab Danesh Institute of Higher Education, Qom*

خلاصه مقاله:
Network security is one of the most challenging issues in network communication world. As network communications grow, vulnerabilities and penetrating attacks are predicted to be as prominent factors. So in order to thwart these attacks an intelligent and powerful intrusion detection system in required. In this paper, a multilayer intrusion detection system is proposed. In first layer, four types of detector are created using genetic algorithm which are used in the second layer to detect some anomalies or abnormal traffic data using Negative Selection Algorithm (NSA) and finally in last layer, the detected anomaly data are classified into four types of attack: DoS, Probe, R2l and U2r. The results show better performance in detecting and classifying new or unseen abnormal data. All experiments are done using KDDCUP99 dataset

کلمات کلیدی:
detector, genetic algorithm, Negative Selection Algorithm (NSA), DoS, Probe, R2l, U2r, KDDCUP99

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/480037