International J. of Engg. Research & Indu.Appls.
ISSN 0974-1518, (IJERIA), Vol.1, No.I (2008), pp.187-197

ANOMALOUS NETWORK INTRUSION PROTECTION SYSTEM USING RULE BASE

S. JEYA & K. RAMAR

Abstract

The field of Intrusion Detection System (IDS) is still developing; the systems that do exist are still not complete, in the sense that they are not able to detect all types of intrusions. Quickly increased complexity, openness, interconnection and interdependence have made computer systems more vulnerable and difficult to protect from malicious attacks. Network intrusion detection system plays a vital role in today's network. The attacks detection can be classified into either misuse or anomaly detection. The misuse detection cannot detect unknown intrusions whereas the anomaly detection can give false positive. Combining the best feature of misuse and anomaly detection one intelligent intrusion detection system (IIDS) is proposed which is able to detect not only the known intrusions but also the unknown intrusions. For detecting the unknown intrusions the proper knowledge base is to be formed after preprocessing the packets captured from the network. The preprocessing is the combination of partitioning and feature extraction. The partitioning of packets is based on the network services and extraction of attack feature is added to the knowledge base. The preprocessed attacks can be classified by using mining classification which will be given to rule builder. Once the unknown intrusions are detected that information's can be added to misuse detector for further detection. The network intrusion detection system should be adaptable to all type of critical situations arise in network.

Key words: Genetic Algorithm, Artificial Intelligence, Network Sniffer, local response and global response.