Abstract

In recent years, with the growth of network technologies and its sizes the ratio of attacks has also increases. An attack is an event which has been designed with the aim to bypass the security parameters such as confidentiality, integrity, and/or availability of a standalone computer system or a network. Sometime attacks may cause of heavy loss for an individual, or an organization. To reduce an effect of attacks, it is good to detects at an early stage as it entered in a system or network. However, since the age of computer network number of researchers and industry communities has proposed a variety of exclusive attack detection algorithms in order to prevent information from such threats but each approach has its own problem in their performance. On the other hand most of the accessible techniques use signature base algorithm, detect only previously identified attack types, fails to detect the new attacks and produce huge false alarms so not be suitable for high pace networks. These issues severely restrict the utility of deterrence system. This paper has considered such issues and proposed a novel attack detection technique which generates low false alarms with enhancing the attack detection rate of known as well as anomaly attacks over the network.
References

1. Frank Kargl, Jörn Maier, Stefan Schlott, Michael Weber – Protecting Web Servers from Distributed Denial of Service Attacks‖ ACM 1-58113-348-0/01/0005. May 1-5, 2001,
18. R. Fei, L. Hu & H. Liang, “Using Density-based Incremental Clustering for Anomaly


29. Prabhjeet Kaur, Amit Kumar Sharma, Sudesh Kumar Prajapat “ Madam ID for intrusion detection using data mining” IJRIM volume 2, issue 2, February 2012


Index Terms

Computer Science

Networks

Keywords

Intrusion Detection System, Security, Data Mining, Feature Extraction.