Abstract

An intrusion detection system (IDS) is a device or software application that monitors network and/or system behavior for malicious activities or policy violations and produces reports to a Management Station. In this project we design and implement an IDS that is a software application and monitor network through a client server approach and to detect users activity we can use a process monitor for intruder detection. Here client application is gather system process and update information over server. Server contains the database and an intelligent algorithm to classify the process patterns. If classified data belongs to the previously detected attack then generate alarm and if the process pattern is not classified as previously then that means it is a new kind of attack and update the current database.

References

- An Artificial Immune Model for Network Intrusion Detection, Jungwon Kim and Peter Bentley Department of Computer Science, University College London Gower Street, London, WC1E 6BT, U. K. Phone: +44-171-380-7329, Fax: +44-171-387-1397 email:{J. Kim, P. Bentley}@cs. ucl. ac. uk
- Testing Network-based Intrusion Detection Signatures Using Mutant Exploits, Giovanni Vigna vigna@cs. ucsb. edu William Robertson wkr@cs. ucsb. edu Davide Balzarotti
IDS with Hybrid ID3 Algorithm

balzarot@cs.ucsb.edu Reliable Software Group University of California, Santa Barbara Santa Barbara, CA 93106
- A Neural Network Based System for Intrusion Detection and Classification of Attacks Mehdi MORADI and Mohammad ZULKERNINE
- The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors Daejoon Jooa,*, Taeho Hongb,1, Ingoo Hanc,2
- Anomaly-based network intrusion detection: Techniques, systems and challenges P. Garc?´a-Teodoro a ,*,J. D´az-Verdejo a, G. Macia´-Ferna´ndez a,E. Va´zquez b a. Department of Signal Theory, Telematics and Communications – Computer Science and Telecommunications Faculty, University of Granada, Granada, Spain b. Department of Telematic Engineering - Universidad Polite´cnica de Madrid, Madrid, Spain
- Neural Network Based Intrusion Detection System for Critical Infrastructures, Ondrej Linda, Todd Vollmer, Milos Manic, Member, IEEE
- A hybrid intrusion detection system design for computer network security, M. Ali Ayd?n*, A. Halim Zaim, K. G?¨okhan Ceylan Department of Computer Engineering, Faculty of Engineering, Istanbul University, 34320 Avcil, Istanbul, Turke
- A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection, Jiankun Hu and Xinghuo Yu, RMIT University D. Qiu, Sai Global Limited Hsiao-Hwa Chen, National Cheng Kung University
- Agent-based Intrusion Detection for Network-based Application Jianping Zeng1 and Donghui Guo2 (Corresponding author: Donghui Guo) Department of Physics, Xiamen University, Fujian 361005, China1 Department of Electronic Engineering, Xiamen University, Fujian 361005, China2 (Email: dhguo@xmu.edu.cn)
- IJCSNS International Journal of Computer Science and Network Security, VOL. 11 No. 8, August 2011 Manuscript received August 5, 2011 Manuscript revised August 20, 2011 Implementing Rule based Genetic Algorithm as a Solution for Intrusion Detection System Shaik Akbar† Dr. K. Nageswara Rao†† Dr. J. A. Chandulal†††, † Assoc. Prof. Dept. of C. S. E SVIET, Nandamuru, Krishna Dist, Andhra Pradesh, India †† Prof & H. O. D, Dept. of C. S. E P. V. P. S. I. T, Vijayawada, Krishna Dist, Andhra Pradesh, India ††† Prof. Dept. of C. S. E GITAM University, Visakhapatnam, Andhra Pradesh, India

Index Terms
**Keywords**

IDS  process monitor  patterns  alarm  database. engines.