Abstract

Web servers and web-based applications are popular attack targets. Web servers are usually accessible through corporate firewalls. The number of reported web application vulnerabilities is increasing dramatically. Thus the task of securing web applications is one of the most urgent. On the other hand traditional protection mechanisms like firewalls were not designed to protect web applications and thus do not provide adequate defense. Current attacks cannot be thwarted by just blocking ports 80 (HTTP) and 443 (HTTPS). Previously known intrusion detection systems are not efficient with more false positive alarms and more time and space complexity. In this research work a new IDS architecture is introduced which detect misconfiguration and intrusion simultaneously. There is also used a RBs (Rule Based System) which take appropriate action accordingly degree of misconfiguration. The RBs consist with predefined rule. This rules guide the system to take appropriate action. Rules are triggered as soon as it received signal for misconfigurations. The architecture designed such a way that it can handle misconfigurations and detection of intrusion simultaneously.
Enhanced Architecture for Misconfiguration and Intrusion Detection using Centralized Rule based System

References

- Nisha Verma, Mohd Husain, Manoj Kumar Shukla, Research on Mobile agent based network intrusion, 2011
- Mueen Uddin, Kamran Khowaja, and Azizah Abdul Rehman, Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents, 2010
- Fakher Ben Ftima, Kamel Karoui, Henda Ben Ghezala, Misconfigurations Discovery Between Distributed Security Components Using the Mobile Agent Approach, ACM New York, NY, USA 2009
- Bhushan Trivedi, Jayant Rajput, Chintan Dwivedi, and Pinky Jobanputra, Distributed Intrusion Detection System using Mobile Agents, 2009
- Sergio Ilarri, Eduardo Mena, Arantza Illarramendi, Using cooperative mobile agents to monitor distributed and dynamic environments, Elsevier Science Inc. New York, NY, USA 2008
- Álvaro Herrero, Emilio Corchado, María A. Pellicer, and Ajith Abraham, Hybrid Multi Agent-Neural Network Intrusion Detection with Mobile Visualization, 2007
- Pradeep Kannadiga and Mohammad Zulkernine, DIDMA: A Distributed Intrusion Detection System Using Mobile Agents, 2005
- Shao-Chun Zhong, Qingfeng Song, Xiao-Chun Cheng, Yan Wang, A Safe Mobile Agent System for Distributed Intrusion detection, 2003

Index Terms

Computer Science

Security
Keywords
Intrusion Detection  Mobile Agent  Network Security