Abstract

Intrusion detection and prevention is one of the most important and fundamental task in an organization’s computer network. Commercially available intrusion detection and prevention systems are costly and overkill for small and medium sized organizations. This paper describes the design and analysis of a network intrusion detection system (NIDS) and network intrusion prevention system (NIPS) using open source tools. The study also describes an open source Database to store the alerts and an open source front end management console application to view the alerts and logs from the proposed Database in any of the modern day web browser. In this particular research Snort was used as an NIDS to detect intrusions and attacks. Snort is a popular open source NIDS with signature based rules for detecting thousands of known attacks. The rules are regularly updated by Snort team to include new attacks and intrusions. SnortSam was used as an NIPS to act upon the alerts detected by Snort. SnortSam blocks the intrusions by sending intruders and attacker’s source IP addresses to firewall in real time. MySQL was used as the Database to store alerts and BASE (Basic Analysis and Security Engine) was chosen as the open source management console application. Juniper Networks switch EX-3200
and Firewall SSG-20 were used as the network devices for connectivity and working of the system. Any other vendor network devices can also effectively be used in design and configuration of the system. The design successfully detected and prevented network intrusions and same can be implemented in any small and medium sized organization for protection of their Computer Networks.

References


Index Terms

Computer Science Networks

Keywords

BASE (Basic Analysis and Security Engine), MySQL, NIDS, NIPS, Snort, Snortsam.