ABSTRACT

The rapid amount of internet growth demanding every aspect of everyday life to utilize the internet according to each aspect's necessity. One of those aspects is corporations. Internet has influenced the performance of corporations in doing its job. An corporate's administrator must be able to secure the internet network from things that can cause detriment such as data loss, hacking, hijacking, and data manipulation. This final project will construct a management system of network security using Open Source Security Information Management (OSSIM) which will help the administrator in handling and securing a network. OSSIM which acts as SIEM (Security Information and Event Management) will be integrated with OSSEC Agent HIDS module as attacks detector (Intrusion Detection System). The OSSIM will presents of detection results in real time log event and graphs which will help administrators to quickly acknowledge the attack.

Keywords: OSSIM, SIEM, OSSEC agent HIDS, Instrusion Detection System