ABSTRAK

IDS (Intrusion Detection System). IDS adalah sebuah sistem yang dapat secara otomatis memonitor kejadian pada jaringan komputer dan dapat menganalisa masalah keamanan jaringan. IDS mampu mendeteksi penyusup dan memberikan respon secara real time. Terdapat dua teknik yang digunakan dalam IDS yaitu, NIDS (Network Based Intrusion Detection System) dan HIDS (Host Based Intrusion Detection System). HIDS memiliki beberapa kelebihan dibandingkan dengan NIDS, sehingga yang akan diimplementasikan kali ini adalah IDS dengan teknik HIDS dengan menggunakan perangkat lunak bernama OSSEC (Open Source Security). Pada percobaan ini PC Server menggunakan sistem operasi Linux Ubuntu 13.10. Pengujian dilakukan pada Local Area Network dengan topologi Star, 4-6 jam selama 6 hari. Berdasarkan percobaan yang telah dilakukan, terdapat total 128.576 peringatan. 51 diantaranya adalah peringatan tentang serangan DoS dan 678 diantaranya adalah peringatan serangan SQL Injection. serta IDS dengan teknik HIDS dapat memantau kejadian pada jaringan dengan baik.

Kata kunci: Keamanan Jaringan, IDS, NIDS, HIDS, OSSEC

ABSTRACT

IDS (Intrusion Detection System). IDS is a system that can automatically monitor events on a computer network and can analyze the network security issues. IDS is able to detect intruders and provide a response in real time. There are two techniques used in IDS, NIDS (Network-Based Intrusion Detection System) and HIDS (Host-Based Intrusion Detection System). HIDS has several advantages compared to the NIDS, so that will be implemented this time is the IDS with HIDS technique using a software called OSSEC (Open Source Security). In this experiment Server PC using the Linux operating system Ubuntu 13:10. Testing is done on a Local Area Network with a star topology, 4-6 hours for 6 days. Based on the experiments that have been conducted, there are a total of 128 576 warnings. 51 of them are warning about DoS attacks and 678 of them are warning SQL Injection attacks. and IDS with HIDS technique can monitor events on the network well.

Keywords: Network Security, IDS, NIDS, HIDS, OSSEC