IMPLEMENTASI DAN ANALISIS PENGAMANAN JARINGAN MENGGUNAKAN SNORT *INTRUSION DETECTION SYSTEM* (IDS) DAN *HONEYPOT*

Fajar Dwi Saputra

Abstrak

Penelitian ini dilakukan untuk membuat sistem yang dapat digunakan untuk mendeteksi gangguan pada sisi sistem kinerja server yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan menganalisis masalah keamanan jaringan. Snort menggunakan dua metode yaitu *knowledge based* atau *misusedetection* yaitu mengenali adanya penyusupan atau serangan dengan cara menyadap paket data kemudian membandingkannya dengan *database rule* yang berisi *signature-signature* serangan dan *behavior based* atau *anomaly based*. Snort IDS ini bekerja dengan cara mendeteksi serangan yang telah dilakukan oleh penyusup (*intruder*). Setelah serangan berhasil terdeteksi, maka serangan tersebut akan dibelokkan ke server palsu (Honeypot). Akibat dari serangan penyusup adalah terjadinya gangguan pada sisi sistem kinerja server. Begitupula pada pemakaian CPU *history* adanya peningkatan kapasitas server 47,5% ketika terjadi serangan. Akan tetapi setelah terjadinya pembelokan, kapasitas server menurun menjadi 13,7%. Setelah dilakukan proses pendeteksian dan pembelokan maka sistem sudah bekerja dengan baik untuk mengamankan suatu jaringan komputer. Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada di dalam *rule* IDS atau tidak. Oleh karena itu, pengelola IDS harus secara rutin memperbaharui *rule*.

Kata Kunci : Snort IDS, CPU History, Honeyd, Kinerja Sistem, penyusup.

IMPLEMENTATION AND ANALYSIS OF NETWORK SECURITY USING SNORT INTRUSION DETECTION SYSTEM (IDS) AND HONEYPOT

Fajar Dwi Saputra

Abstract

This study was conducted to create system that can be used to detect intruder on the server performance system that works automatically to monitor events on computer networks and analyze network security issues. Snort uses two methods of knowledge based or misusedetection that recognize their intrusion or attack by way of intercepting data packets and then compares it with a database rule that contains an attack signature and signature-based or behavior-based anomaly. IDS Snort works by detecting attacks that have been carried out by the intruder. After a successful attack is detected, then the attack will be diverted to a fake server (Honeypot). As a result of the attack the intruder is interference with the performance of server side system. Likewise, CPU usage history to an increase of 47.5% server capacity when the attack occurred. But after the deflection, server capacity decreased to 13.7%. After the detection process and the deflection of the system is already working well to secure a computer network. The attack can be detected or not depending on the pattern of the attacks in the IDS rule or not. Therefore, managers should regularly update the IDS rule.

Keywords : Snort IDS, CPU History, Honeyd, System Performance, Intuder.