Analisis Performa *Network Intrusion Detection System* (NIDS) Menggunakan Metode *Signature Based* Dalam Mendeteksi Serangan *Denial of Service* (DoS) Berbasis *UDP Flooding*

Muhammad Rien Suryatama Idrus

ABSTRAK

Cloud computing telah menjadi tren teknologi yang digunakan oleh berbagai kalangan terutama para pelaku *startup* dan perusahaan besar. Beberapa kelebihan yang ditawarkan *cloud computing* seperti kemudahan untuk membuat layanan *cloud* sendiri, hemat biaya infrastruktur dan fleksibel dalam menambah atau mengurangi kapasitas layanan sesuai dengan kebutuhan. Terlepas dari kelebihan-kelebihan tersebut, aspek keamanan *cloud computing* menjadi salah satu faktor yang harus diperhatikan oleh perusahaan. Penggunaan antivirus dan *firewall* belum menjamin sistem *cloud* sepenuhnya aman. Selain itu keterbatasan administrator dalam memonitor *traffic* dan serangan di seluruh bagian jaringan *cloud* menjadi kendala dalam pengelolaan *cloud computing*. Salah satu solusi untuk meningkatkan keamanan jaringan, memonitor serta mengawasi *traffic* serangan pada *cloud computing* adalah *Network-based Intrusion Detection System* (NIDS). NIDS merupakan salah satu jenis *Intrusion Detection System* (IDS) yang dapat melakukan pemantauan terhadap serangan serta *traffic* pada seluruh bagian jaringan. *Signature based* adalah salah satu metode yang dapat digunakan NIDS dalam mengidentifikasi setiap paket data yang keluar dan masuk ke jaringan. Pada penelitian ini, penulis melakukan uji performa NIDS dengan metode *Signature Based* dalam mendeteksi serangan DoS berbasis *UDP Flooding*. Penelitian ini juga melakukan analisis terhadap hasil dan evaluasi performa NIDS untuk mengetahui kinerja diterapkannya NIDS dan keakuratan NIDS dalam mengklasifikasikan serangan.

Kata Kunci : IDS, *Network Intrusion Detection System*, NIDS, *Cloud* Computing, Signature Based

Analysis Performances of Network Intrusion Detection System (NIDS) Using Signature Based Method in Detecting Denial of Service (DoS) Based on *UDP Flooding* Attack

Muhammad Rien Suryatama Idrus

Abstract

Nowadays, *cloud* computing has become a new trend technology used in various areas, especially in startup and big companies. *Cloud* computing offers some advantages such as the easiness to create their own *cloud* services, cost-effective infrastructure and flexible to increase or decrease the capacity of the service in accordance with the requirements. Apart from these advantages, the security aspects of *cloud* computing is becoming one of the factors that must be considered by the company. The use of antivirus and firewall doesn't guarantee the *cloud* system is fully secure. Besides that, the limitation of administrator to monitor traffic and attacks throughout the *cloud* network become a constraint in *cloud* computing management. One solution to improve network security, traffic monitoring and overseeing attacks on *cloud* computing using Network-based Intrusion Detection System (NIDS). NIDS is one type of Intrusion Detection System (IDS) which can monitor the attacks and traffic throughout the network. Signature Based is one method that can be used NIDS to identify each packet of data in or out to the network. In this research, the author conducted performances test NIDS with Signature Based method based on *UDP Flooding*. This research also perform conducted analysis of the result and performance evaluation of NIDS on *cloud* computing. The aim to determine the performance of NIDS and the accuracy of NIDS in classifying attacks.

Kata Kunci : IDS, *Network Intrusion Detection System*, NIDS, *Cloud* Computing, Signature Based