INTISARI

ANALISIS STRUKTUR BASISDATA NO-SQL UNTUK KEBUTUHAN SISTEM KEAMANAN JARINGAN BERBASIS HONEYNET

Keamanan jaringan merupakan sebuah kebutuhan untuk menjaga sistem agar tetap aman dari penyerangan pihak yang tidak bertanggung jawab. *Honeypot* merupakan salah satu utilitas yang bisa digunakan untuk mengelabuhi para penyerang tersebut. Sehingga ketika *honeypot* terpasang pada sebuah sistem, seolah-olah penyerang berhasil melakukan aksinya, tetapi ternyata tidak, dan sistem akan tetap terjaga. Namun, banyaknya serangan yang ada membuat *honeypot*, khususnya yang menggunakan sensor dengan spesifikasi dan kapasitas rendah, akan mengalami penurunan performa karena kapasitas penyimpanan yang penuh dengan data-data penyerangan yang disimpan pada sensor *honeypot* itu sendiri. Selain itu, jumlah serangan yang sangat banyak akan menyulitkan admin keamanan jaringan untuk menganalisis data tersebut. Untuk itu, dibutuhkan sebuah struktur basisdata yang bisa menampung *log* penyerangan dari beberapa tipe *honeypot* sekaligus untuk mempermudah analisis data penyerangan dari semua tipe *honeypot* yang terpasang. Untuk menampung data yang sangat besar tersebut dibubutuhkan sebuah basisdata dengan orientasi berbasis dokumen seperti MongoDB. Basisdata tersebut dirancang untuk menyimpan, mengambil, dan mengolah data dengan jumlah yang sangat besar, di mana pada penelitian ini data yang didapat dari *honeypot* akan memberikan jumlah data yang sangat besar. *Honeypot* yang digunakan dalam penelitian ini adalah Dionaea.

Kata Kunci: Basisdata, *Honeypot, No-SQL,* Keamanan Jaringan

ABSTRACT

ANALYSIS OF ORIENTED DOCUMENT DATABASE STRUCTURE FOR DIONAEA HONEYPOT NETWORK SECURITY SYSTEM

Network security is a nessecity to keep the system safe from being attacked by the irresponsible parties. Honeypot is one of the utilities which can be used to deceive the attackers. When honeypot installed in a system, the attacker may feel that they're able to break the system. But actually, its just the honeypot that they success to break while the primary system is safe. However, the large number of the attacks that entered the system may decrease the system performance because the attack logs stored on the honeypot sensor itself can make the storage full in a short period. In addition, the large number of attacks will make it difficult for the admins to analyze the data. For this reason, a basisdata structure that meet the requirements to save the logs from several types of honeypot is needed. MongoDB as a document-oriented basisdata may be the choice to accommodate this large number of attack logs. The basisdata is designed to store, retrive, and process large amount of data. In this study, the data come from honeypot. The honeypot used in this study is Dionaea.

***Keywords**: Database, Honeypot,* MongoDB, *Network Security*