INTISARI

PROYEK AKHIR

PENERUSAN DATA SERANGAN PADA *HONEYPOT* KE *SERVER* BASIS DATA SECARA PERIODIK MENGGUNAKAN PYTHON

Abstrak — Salah satu bentuk teknologi yang berkaitan erat dengan keamanan pada jaringan adalah *honeypot.* Berfungsi untuk menjebak penyerang yang berasal dari dalam dan luar jaringan, mencatat serangan tersebut, kemudian menyimpannya ke dalam suatu log yang memiliki struktur basis data *relational*. Data serangan tersebut dapat dimanfaatkan untuk keperluan analisa data. Pada cara tradisional, administrator jaringan mengambil data tersebut ketika *honeypot* sudah tidak mampu menampung data serangan terbaru dan pengambilan data serangan masih menggunakan protokol *File Transfer Protocol* (FTP) dan *Secure Shell* (SSH). Pengambilan data serangan tersebut kurang efisien. Sistem penerusan data serangan *honeypot* menuju ke *server* merupakan solusi yang tepat untuk mengatasi masalah tersebut. Proyek akhir ini akan membuat utilitas penerusan data serangan pada *honeypot* menuju ke *server* dengan memanfaatkan *framework* Flask, untuk mengubah data serangan yang memiliki struktur *relational* ke dalam struktur *JavaScript Object Notation* (JSON) dan *library* pymongo untuk menghubungkan ke basis data MongoDB. Pengujian yang dilakukan terhadap utilitas tersebut adalah menggunakan beberapa modul yang terdapat pada *metasploit framework*. Utilitas ini dapat dimanfaatkan sebagai penerusan data serangan pada *honeypot* sehingga analisis data terhadap data serangan *honeypot* dapat dilakukan lebih efisien.

Kata Kunci : *Honeypot*, SQLITE, JSON, MongoDB, Python, Flask

ABSTRACT

Forwarding Attack Data on Honeypot to a Database Server Using Python Periodically

Abstract — One form of technology that is closely related to network security is a honeypot. Serves to trap attackers who come from inside and outside the network, record the attack, then save it in a log which has a relational database structure. The attack data can be used for data analysis purposes. In the traditional way, network administrators retrieve this data when the honeypot is no longer able to accommodate the latest attack data and the attack data retrieval is still using the File Transfer Protocol (FTP) and Secure Shell (SSH) protocols. Retrieval of attack data is less efficient. The honeypot attack data forwarding system to the server is the right solution to solve this problem. This final project will create a data forwarding utility on the honeypot to the server by utilizing the Flask framework, to convert the attack data which has a relational structure into a JavaScript Object Notation (JSON) structure and the pymongo library to connect to the MongoDB database. Tests that will be carried out on these utilities is to use several modules contained in the metasploit framework. This utility can be used to forward attack data to the honeypot, so that data analysis of honeypot attack data can be carried out more efficiently.

Keywords : *Honeypot*, *SQLITE, JSON, MongoDB, Python, Flask*