INTISARI

IMPLEMENTASI ELK STACK SEBAGAI VISUALISASI SERANGAN PADA HONEYPOT DIONAEA

Poppy Yohana Sinaga
18/425700/SV/14842

Internet berkembang sangat pesat, namun memberikan kelemahan yang dapat dimanfaatkan oleh penyerang. Honeypot merupakan komputer atau sistem yang sengaja dibuat untuk menarik perhatian penyerang agar seolah-olah penyerang tersebut berhasil masuk ke suatu jaringan dan berhasil mendapatkan data padahal data itu bukan data yang sebenarnya. Dengan pemasangan Honeypot dapat memberikan informasi mengenai penyerang karena adanya log serangan. Seiring bertambahnya waktu, data informasi serangan pada log juga akan bertambah, sehingga diperlukan sebuah sistem yang dapat menganalisis, menampilkan data dengan cepat. Penelitian ini bertujuan untuk mempermudah pekerjaan *Cyber Analyst* dalam mengetahui sejauh mana serangan yang dilakukan oleh penyerang. Data serangan yang digunakan dimulai dari tanggal 23 Februari hingga 9 Maret 2022. Dari data ini, dicari 10 besar layanan yang mendapatkan serangan terbanyak, kemudian 3 diantaranya divisualisasikan berdasarkan aktivitas yang terekam pada Honeypot Dionaea sehingga menghasilkan sebuah informasi mengenai penyerang. ELK Stack merupakan komponen yang terdiri dari Elasticsearch, Logstash, dan Kibana dapat menjadi solusi dari permsalahan yang ada. Data serangan yang disimpan dalam MongoDB server dikirimkan melalui Logstash menuju Elasticsearch kemudian ditampilkan Kibana. ELK Stack dapat mempermudah pekerjaan Cyber Analyst dalam mengetahui sejauh mana serangan yang dilakukan penyerang. *Service* SMB yang hanya *connection* sampai 99,59% dan sampai tahap unggah file 0,41%. *Service* MySQL yang hanya *connection* sampai 10,01%, sampai tahap *log in* 13,29%, sampai tahap mengirimkan perintah 75,54% dan sampai tahap mengunggah *file* 1,16%. *Service* MsSQL yang hanya *connection* sampai 7,15% dan sampai tahap *log in* 92,85%.

Kata kunci: ELK Stack, Serangan, *Port Scanning*, Honeypot Dioanea

ABSTRACT

THE IMPLEMENTATION OF ELK STACK FOR ATTACK VISUALIZATION ON HONEYPOT DIONAEA

The Internet is growing very rapidly but provides weaknesses that the attacker can utilize. A Honeypot is a computer or system that is intentionally created to attract the attention of attackers so that it seems as if the attacker managed to enter a network and managed to get data when the data was not the actual data. The installation of Honeypot provides information about the attacker because of the attack log. Over time, the attack data in the log will also increase, so we need a system that can analyze and display data quickly. This study aims to make the work of Cyber Analysts easier in knowing the extent of attacks carried out by attackers. The attack data is used starts from 23 February to 9 March 2022. From this data, the top 10 services are searched for the most attacks, then 3 of them are visualized based on activity recorded on Dionaea Honeypot to gain information about the attacker. ELK Stack is a component consisting of Elasticsearch, Logstash, and Kibana can be a solution. The attack data stored on the MongoDB server is sent via Logstash to Elasticsearch then it is visualized by Kibana. ELK Stack makes it easier for Cyber Analysts to find out the extent of the attacks carried out by attackers. SMB service only connects up to 99.59% and download stage up to 0.41%. MySQL service which only connects up to 10.01%, until the login stage is 13.29%, until the stage of sending commands 75.54%, and until the download stage 1.16%. MsSQL service only connects up to 7.15% and logs in at 92.85%.

Keyword: *ELK Stack, Attack, Port Scanning, Honeypot Dionaea*