ABSTRAK

Dalam istilah komputer, Honeypot merupakan sebuah metode mekanisme keamanan untuk mendeteksi, menghadang, atau dalam beberapa cara mampu melawan aksi yang tidak sah pada komputer. Honeypot termasuk dalam kategori *intrusion prevention system* (IPS) yang banyak digunakan pada komputer guna mengamankan komputer tersebut. Honeypot dapat membantu dalam mempelajari cara penyerang melakukan serangan karena di dalam Honeypot di bisa mengetahui apa saja yang di lakukan penyerang untuk melakukan serangan. Dari semua kemampuan Honeypot itu, Honeypot memiliki satu kekurangan dimana *User Interface* yang kurang kurang ramah untuk manusia, tidak ada penjelasan total jumlah Log yang masuk, serta tidak ada waktu dan tanggal Log tersebut diterima.

Oleh karena itu pada Tugas Akhir ini ingin mencoba menggunakan aplikasi Elasticsearch dan Kibana untuk membuat hasil dari rekaman Honeypot tersebut lebih ramah bagi pengguna. Dengan menggunakan Elasticsearch sebagai mesin *database* dan Kibana sebagai aplikasi untuk menampilkan hasil dari Elasticsearch tersebut. Maka dapat membuat data hasil Honeypot lebih mudah untuk di baca dan dapat di simpan oleh pengguna, sehingga mampu mempermudah dalam menggunakan Honeypot tersebut. Pengujian Dilakukan dengan melakukan serangan siber terhadap honeypot, membandingkan hasil Log dari serangan tersebut, serta menganalisa *resource* server yang di gunakan ketika terjadi serangan.

Hasil Pengujian dapat disimpulkan Elasticsearch mampu menerima semua data Log dari Honeypot. Dimana hasil perbandingan data Log yang ada pada honeypot sama persis dengan yang ada pada Kibana. Dan dari analisa *resource* server didapatkan bahwa penggunaan Elasticsearch untuk membantu *monitoring* Log membebani server karena Elasticsearch menggunakan banyak *resource* server. Elasticsearch menggunakan hingga 86% *resource* server. Dimana hanya 17% penggunaan *resource* jika Honeypot berjalan tanpa Elasticsearch.

Kata Kunci: *Honeypot, Elasticsearch, Kibana, Docker.*