ABSTRAK

Server merupakan jantung bagi beberapa *platform* sekarang seperti *website*, *game*, DHCP, *mail*, *cloud*, *database*, dan masih banyak lagi yang dapat memenuhi kebutuhan pengguna. Maka dari itu keaamanan merupakan hal yang sangat krusial agar mengurangi persentase terjadinya serangan, atau kebocoran data terutama pada *server database*. Pencegahan dari adanya serangan ini menggunakan metode *vulnerability asssessment* menggunakan ELK *Stack* yang akan di terapkan pada *server database*. Dengan menggunakan uji statistika dan *three sigma* pada hasil grafik ELK *Stack* untuk menguji *vulnerability assesment* pada penelitian Tugas Akhir ini.

ELK *Stack* bekerja secara independen dengan memecah menjadi beberapa bagian. Diawali dari *Elasticsearch, Logstash*, dan *Kibana* yang mempunyai fungsinya masing-masing. Mempunyai alur pengerjaan dengan dimulai pada *log* yang akan dicari oleh *Elasticsearch*, juga *Logstash* yang kemudian memilah hasil pencarian *log* yang nantinya akan ditampilkan hasil grafik daripada *Elasticsearch* dan *Logstash* pada *Kibana.* Sehingga hasil grafik pada *Kibana* dapat diuji secara statistik apakah ELK *Stack* dapat digunakan untuk *vulnerability assessment tools*.

Pengujian dalam implementasi ELK *Stack* ini pada *vulnerability assessment tools* menggunakan metode pengujian statistik dengan mencari nilai standar deviasi, dan nilai *three sigma.* Maka pada hasil pengujian ini mendapatkan hasil nilai rata-rata standar deviasi sebesar 1.266,9 dari 5 fitur *dataset.* Dari hasil pengujian ini maka implementasi pada ELK *Stack* untuk *vulnerability assessment tools* hanya mampu membaca *log* namun tidak dapat memindai *log* tersebut.

Kata Kunci: Dataset, DDoS, ELK Stack, Security, Server, Vulnerability Assessment.