

ABSTRAK

Dengan semakin berkembangnya teknologi, media penyimpanan berbasis *database server* menjadi semakin sering digunakan terutama untuk keperluan perusahaan ataupun bidang akademik. Penggunaan *database server* ini sangat rawan dengan ancaman keamanan *data* sehingga diperlukannya pendeteksi kerentanan yaitu *ELK Stack*. Pemasangan aplikasi sekuritas merupakan hal penting untuk mengurangi risiko yang dimiliki oleh penyedia layanan sehingga keamanan *data* yang dimiliki oleh penyedia layanan dapat terjaga.

Penggunaan *ELK Stack* dapat meningkatkan keamanan karena dapat memberitahukan apabila ada *data log* yang rentan terhadap serangan ataupun pencurian sebuah *data*. *ELK Stack* ini mampu mengurangi ancaman dengan melakukan filter pada *data log* yang diolah oleh *Logstash* berdasarkan *data* yang diterima oleh *Elasticsearch* pada saat mengambil *data* dari *server* yang telah dipasang *ELK Stack*. Dengan tersaringnya *data* yang ada maka akan dikategorikan menjadi *data* yang rentan dan tidak lalu informasi itu akan ditampilkan pada menu utama *Kibana* sehingga dapat menindaklanjuti ancaman.

Pengujian yang dilakukan pada *ELK Stack* sebagai *Vulnerability Assessment Tools* yang mendapatkan hasil bahwa penggunaan aplikasi *ELK Stack* ini memiliki fungsi untuk membaca *log*. Pengujian selanjutnya *data* yang telah diolah pada *ELK Stack* dilakukan uji statistik dengan menggunakan metode *3 Sigma Rule*. Hasil yang didapatkan dari pengujian statistika berdasarkan empat kali pengujian didapatkan hasil 100% dikarenakan seluruh pengujian memenuhi syarat yaitu 99,7% *data* berada dalam tiga bagian *sigma*.

Kata Kunci: *Cloud, ELK Stack, Elasticsearch, Kibana, Logstash.*