

BAB VI

KESIMPULAN DAN SARAN

Pada tahapan ini akan dijelaskan mengenai kesimpulan dan saran dalam penelitian perancangan dan implementasi dashboard monitoring dan analisa serangan aplikasi web menggunakan ELK Stack.

6.1 Kesimpulan

Kesimpulan yang didapatkan dari penulis dalam penelitian ini yaitu ;

1. Dashboard monitoring dihasilkan dari log yang didapatkan snort dengan mendeteksi serangan – serangan yang terjadi pada sebuah web aplikasi. Disini snort berperan sebagai host base IPS/IDS dengan melindungi seluruh perangkat dari server web aplikasi tersebut. Selanjutnya serangan yang sudah dideteksi oleh snort akan dicatat kedalam file log dan file tersebut akan melakukan komunikasi dengan ELK Stack melalui perantara logstash, didalam logstash terjadi pipelining proses yang mana log serang akan dikirimkan kedalam elasticsearch untuk proses indexing dan penyimpanan, setelah berubah menjadi index lalu log tersebut akan terpecah menjadi JSON dan menghasilkan parameter – parameter yang akan digunakan oleh kibana untuk kebutuhan visualisasi
2. Efektifitas dari rancangan sistem dashboard monitoring menggunakan ELK Stack mendapatkan masing – masing hasil dari nilai efektivitas yang dilakukan terhadap alat pendeksian yaitu snort sebesar 100 % dan untuk pengujian efektivitas dari penggunaan dan kelayakan mendapatkan nilai sebesar 96,82 %. Hasil ini tentunya akan menjadi catatan sebagai bahan evaluasi untuk meningkatkan kinerja dari sistem yang sudah dirancang agar lebih baik lagi.

6.2 Saran

Berdasarkan dengan penelitian yang telah dibuat, maka penulis mendapatkan beberapa saran yang nantinya dapat digunakan dalam langkah penelitian selanjutnya.

1. Penelitian ini nantinya dapat dikembangkan pada web aplikasi nyata atau production yang digunakan
2. Penelitian ini nantinya dapat dikembangkan agar dapat mendeteksi lebih banyak macam macam jenis serangan jaringan terutama pada aplikasi web
3. Penelitian ini nantinya dapat dikembangkan dan diuji kembali dengan perangkat IDS yang lain, serta dengan menggunakan data yang lebih kompleks lagi
4. Penelitian ini nantinya dapat dimaksimalkan kembali dalam memvisualisasikan dalam diagram maps untuk memvisualisasikan lokasi dan tempat kejadian serangan



STT - NF