BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan saat ini WLAN telah mengubah cara Internet yang digunakan di dunia yang bermula menggunakan kabel menjadi tanpa kabel (nirkabel). WLAN mencakup area skala kantor kecil hingga skala kampus besar, untuk memaksimalkan keamanan jaringan, organisasi perlu berfokus pada ancaman yang menimbulkan risiko besar. Berdasarkan data https://purplesec.us/resources/cyber-security-statistics/ pada tahun 2018 terdapat 80.000 serangan per hari atau lebih dari 30 juta serangan per tahun. 21% dari semua file tidak dilindungi dan 41% perusahaan memiliki lebih dari 1.000 file sensitif. 70% organisasi mengatakan bahwa mereka yakin risiko keamanan mereka meningkat secara signifikan pada tahun 2017. 69% organisasi tidak percaya bahwa ancaman yang mereka lihat dapat diblokir oleh perangkat lunak anti-virus mereka. 43% dari serangan siber menargetkan bisnis kecil dan 47% bisnis kecil pernah mengalami serangan siber. 3 dari 4 bisnis kecil mengatakan bahwa mereka tidak memiliki personel yang memadai untuk menangani keamanan IT.

Contoh serangan yang dapat terjadi adalah serangan deauthentication dimana serangan berada pada MAC Address pada jaringan yang memanfaatkan protokol 802.11, serangan deotentikasi dapat ditargetkan ke satu pengguna dengan mengirimkan frame sumber palsu yang mengarah ke host yang ingin mereka putuskan atau dapat menargetkan seluruh jaringan dengan membroadcast pada

BSSID Access Point. Meskipun serangan deotentikasi bukan kerentanan yang paling berbahaya dalam protokol, serangan tersebut dapat digunakan sebagai permulaan untuk serangan yang lebih besar seperti evil twin guna mendapatkan informasi yang cukup untuk serangan yang memungkinkan mendapat kendali penuh terhadap jaringan.

Bisnis kecil banyak menggunakan jaringan wireless pada kantor mereka, sehingga rentan terjadi serangan pada jaringan wireless mereka. Dengan menganalisa log maka akan memudahkan untuk menganalisa serangan yang tejadi pada jaringan mereka. *Logging* membantu menyelidiki dan mendiagnosis masalah untuk melakukan perbaikan jika terdapat kerentanan pada sistem. Log tidak hanya menemukan masalah tetapi juga mencari data yang diperlukan. Pada jaringan terdapat log yang menyimpan kinerja yang berjalan dalam komunikasi jaringan. Seringkali penyerang melakukan penyerangan terhadap komunikasi jaringan melalui Wireless fidelity (WiFi), ada beberapa tipe keamanan pada wireless sebagai protokol autentikasi yang sah. Salah satunya adalah WPA2-PSK AES yeng menggunakan autentikasi berupa password[1], dengan demikian pengguna WiFi akan merasa aman karena jaringan yang digunakan terdapat enkripsi dan autentikasi. Ketika terjadi serangan pada jaringan Wireless akan tersimpan aktivitas serangan tersebut pada log, karena sebagian besar log dipusatkan di suatu tempat sehingga dapat melihat aliran prosedur yang harus dilakukan[2].

Perusahaan di masa kini perlu membuat deteksi serangan pada wireless dengan melihat log yang ada pada jaringan tersebut. Untuk mendapatkan log serangan pada jaringan akan menggunakan Raspberry Pi sebagai sensor dan

menggunakan tools seperti airmon-ng dan tshark. Dengan log tersebut dapat diselidiki apakah telah terjadi serangan atau tidak. Untuk menganalisis log tersebut secara efisien dan mudah dimengerti akan menggunakan ELK yaitu Elasticsearch, Logtash, dan Kibana[3]. Sistem manajemen log yang dibangun atas tumpukan ELK bermanfaat untuk menganalisis kumpulan data log yang besar memberikan kemudahan untuk pemantauan melalui antarmuka interaktif[3].

Dengan menggunakan Raspberry Pi sebagai sensor akan mempermudah, karena Raspberry Pi memiliki dimensi yang kecil dan dapat menjalakan sistem operasi seperti Kali Linux, Ubuntu, Raspbian. Karena untuk mendapatkan log pada penelitian ini membutuhkan sistem operasi yang dapat melakukan scanning pada jaringan. ELK (Elasticsearch, Logtash, dan Kibana) akan mempermudah dalam menganalisis log yang telah ada pada jaringan, karena ELK memberikan antarmuka yang interaktif sehingga mempermudah administrator melihat serangan yang terjadi pada jaringan tersebut. Dengan ELK, log dapat disesuaikan dengan keinginan administrator. Log akan dikonversi dalam bentuk tabel, grafik, serta visualisasi.

1.2 **Rumusan Masalah**

Berdasarkan latar belakang diatas, dapat dirumuskan sebuah perumusan masalah yaitu: "Bagaimana cara mengolah dan memanajemen log serangan pada jaringan Wireless agar mudah dipahami oleh administrator jaringan?"

1.3 **Batasan Masalah**

Berikut batasan masalah pada penulisan tugas akhir ini antara lain :

a. Peneliti mencakup analisis, perancangan, dan implementasi menggunakan ELK
b. Menangkap log pada jaringan menggunakan tools tshark.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah :

a. Membuat deteksi serangan deauthentication menggunakan Raspberry Pi sebagai sensor serangan
b. Mengoptimalkan log yang didapatkan dengan memvisualisasikan pada tabel ataupun grafik menggunakan ELK

1.5 Sistematika Penulisan

Berikut merupakan rincian dari sistematika penulisan laporan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi mengenai uraian latar belakang, perumusan masalah, batasan masalah, maksud dan tujuan, manfaat penelitian dan metode penelitian.

BAB II LANDASAN TEORI

Menguraikan teori – teori yang relevan yang mendasari pembahasan pemecah masalah yang berhubungan guna mendukung dalam membuatan tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab metodologi penelitian ini menjelaskan tentang pengertian dari metode dan alat yang digunakan untuk mengembangkan suatu sistem kemanan pada jaringan.

BAB IV HASIL DAN PEMBAHASAN

Membahas tentang implementasi dan hasil dari sistem yang dibangun, serta pelaksanaan uji coba dan evaluasi dari hasil uji coba.

BAB V PENUTUP

Berisi bahasan terkait kesimpulan dan saran mengenai tugas akhir ini untuk pengembangan sistem jaringan selanjutnya.