

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi infrastruktur jaringan pada industri saat ini sangat berkembang dan cepat, hampir semua industri dan perusahaan memanfaatkannya sebagai alat pendukung teknologi informasi yang mereka gunakan. Dengan berkembangnya perangkat jaringan, maka sangat dibutuhkannya suatu sistem untuk manajemen perangkat yang handal, sehingga setiap perangkat dapat dipantau sesuai kinerja perangkat-perangkat jaringan yang diterapkan (Wulandoro, Nurkahfi, & Fitriyani, 2016). Sistem monitoring jaringan merupakan alat untuk mengelola, menganalisa dan memantau perangkat-perangkat jaringan berbasis *Internet Protocol (IP)* yang digunakan pada *administrator* jaringan dalam mengawasi dan mengatur keadaan sistem dan perangkat jaringan (Pratama, Munadi, & Hafidudin, 2017).

Jaringan informasi merupakan infrastruktur jalur pertukaran informasi digital telah berkembang sedemikian pesatnya. Perkembangan ini sayangnya juga diikuti oleh penambahan jumlah ancaman terhadap keamanan jaringan. Aktivitas –aktivitas digital yang melakukan tindakan kejahatan yang biasa dikenal seperti, *hacking*, *malware* dalam bentuk *virus*, *spyware*, *trojan*. Dalam sistem jaringan pasti ditemui kekurangan - kekurangan yang sering muncul, diantaranya adalah gangguan dari dalam berupa virus atau jaringan komputer yang bermasalah dan gangguan dari luar bisa berupa semua bentuk attacking network system .Dari gangguan - gangguan yang sering terjadi pada sistem jaringan, bentuk

gangguan dari luar sangat berbahaya. Gangguan sistem jaringan dari dalam bisa saja karena ada otoritas yang menghendaki perbaikan sistem ataupun pengolahan data sistem sehingga meninggalkan gangguan berupa virus ataupun koneksi yang down, akan tetapi gangguan dari luar adalah tindakan diluar otoritas yang tujuannya lebih pada perusakan dan pencurian data. Semua serangan ini bersifat merugikan, karena informasi yang seharusnya menjadi sangat tertutup bisa diambil oleh yang tidak bertanggung jawab. Serangan - serangan tersebut juga masih sangat berpotensi besar untuk berkembang dan semakin bervariasi.

Mengacu dari beberapa fakta yang ditemukan seperti tindakan yang mengancam terhadap keamanan jaringan sehingga diperlukannya sebuah operasi yang bisa mengawasi ancaman – ancaman yang menyerang terhadap jaringan kita. Operasi ini yang biasa dikenal sebagai SOC (Security Operation Centre) yang dapat melakukan korelasi antara informasi yang dikumpulkan dari berbagai solusi keamanan sehingga kita bisa melakukan analisa terhadap masalah yang timbul atau ancaman yang terjadi dengan jaringan kita.

Dalam penerapan SOC (Security Operation Centre) ini membutuhkan sebuah sistem untuk mendapatkan informasi – informasi ancaman pada jaringan tersebut, penulis menggunakan sistem *Security Onion* sebagai sistem yang digunakan dalam penelitian ini.

Berdasarkan latar belakang diatas, perancangan sistem SOC (*Security Operation Centre*) ini bertujuan untuk mendapatkan informasi – informasi yang

terjadi pada jaringan sehingga kita bisa menganalisa terhadap masalah yang terjadi atau timbul pada jaringan kita. Dengan demikian, penulis telah menetapkan topik skripsi ini dengan judul “**Analisa dan Perancangan Sistem Security Operation Centre Menggunakan Security Onions**”.

1.2 Rumusan Masalah

Berlandaskan pada uraian latar belakang yang sudah dibahas sebelumnya, maka rumusan masalah pada penelitian ini adalah:

1. Bagaimana menganalisa keamanan jaringan dengan menggunakan Security Onions.
2. Bagaimana merancang sistem keamanan jaringan dengan menggunakan Security Onions.
3. Bagaimana menguji keamanan jaringan dengan menggunakan Security Onions.

1.3 Batasan Masalah

Agar pembahasan topik penelitian lebih fokus dan terarah serta dapat mempermudah peneliti untuk mengetahui dan mengukur perkembangan dan peningkatan penelitian, maka peneliti membuat batasan masalah pada penelitian ini, yaitu:

1. Area penelitian akan terbatas pada penyelidikan analisa keamanan jaringan dengan menggunakan Security Onions.
2. Penelitian hanya berlingkup sistem monitoring jaringan dengan menggunakan sistem Security Onions.

1.4 Tujuan Proyek

Tujuan tugas akhir dengan topik “Analisa dan Perancangan Security Operation

Centre Menggunakan Security Onions” tersebut mempunyai tujuan antara lain:

1. Agar kita dapat memonitoring keamanan jaringan.
2. Menambah ilmu pengetahuan dengan merancang sebuah sistem keamanan jaringan dengan menggunakan Security Onions.
3. Sebagai syarat kelulusan Strata 1 (S-1) di Universitas Internasional Batam.
4. Agar penulis mampu mempraktekkan pengetahuan dan wawasan penulis tentang perancangan sistem Security Operation Centre Menggunakan Security Onions.

1.5 Manfaat Proyek

Adapun manfaat dari tugas akhir Analisa dan Perancangan Security Operation

Centre Menggunakan Security Onions, yaitu:

1. Bagi *User*
 - a. Mengedukasi masyarakat terutama perusahaan, instansi dan tempat lainnya yang sistem security operation centre dengan menggunakan security onions.
 - b. Memberikan informasi kepada masyarakat terutama perusahaan, instansi dan tempat lainnya mengenai sistem security operation centre ini dapat membantu dalam pemantauan jaringan.
2. Bagi Penulis
 - a. Meningkatkan pengetahuan terkait sistem monitoring jaringan yang lebih dalam.

- b. Menyelesaikan proyek mata kuliah tugas akhir dalam perkuliahan.

1.6 Sistematika Pembahasan

Berikut merupakan sistematika pembahasan dalam penelitian yang dibuat secara singkat:

BAB I PENDAHULUAN

Bab ini menguraikan secara singkat, jelas dan padat mengenai ringkasan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan proyek, manfaat proyek dan sistematika pembahasan laporan tugas akhir.

BAB II TINJAUAN PUSTAKA

Pada bagian ini berisi teori, temuan, dan bahan penelitian sebelumnya yang relevan dengan penelitian ini. Landasan teori yang ada diperoleh dari berbagai referensi yang dijadikan dasar melakukan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan tentang desain, metode, atau pendekatan yang akan digunakan dalam menjawab permasalahan penelitian untuk mencapai tujuan penelitian, serta tahapan penelitian secara rinci, singkat dan jelas.

BAB IV IMPLEMENTASI

Bab ini akan menguraikan tentang implementasi penelitian. Menjabarkan implementasi perancangan security operation centre yang telah di analisis, direncanakan dan memuat pembahasan tentang hasil dari penelitian yang telah dilakukan.

BAB V PENUTUP

Bab ini merupakan bab penutup yang isinya terdiri atas kesimpulan dan saran dari keseluruhan laporan tugas akhir ini, temuan-temuan yang didapatkan dari hasil analisa serta pembahasan tentang sistem monitoring jaringan.



Universitas Internasional Batam