BAB I

PENDAHULUAN

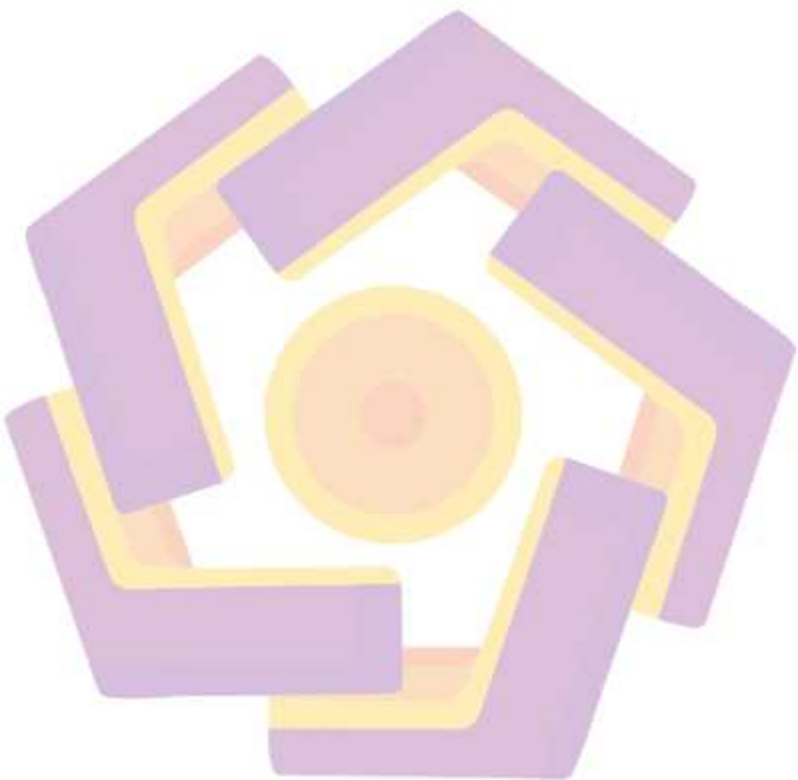
1.1 Latar BelakangMasalah

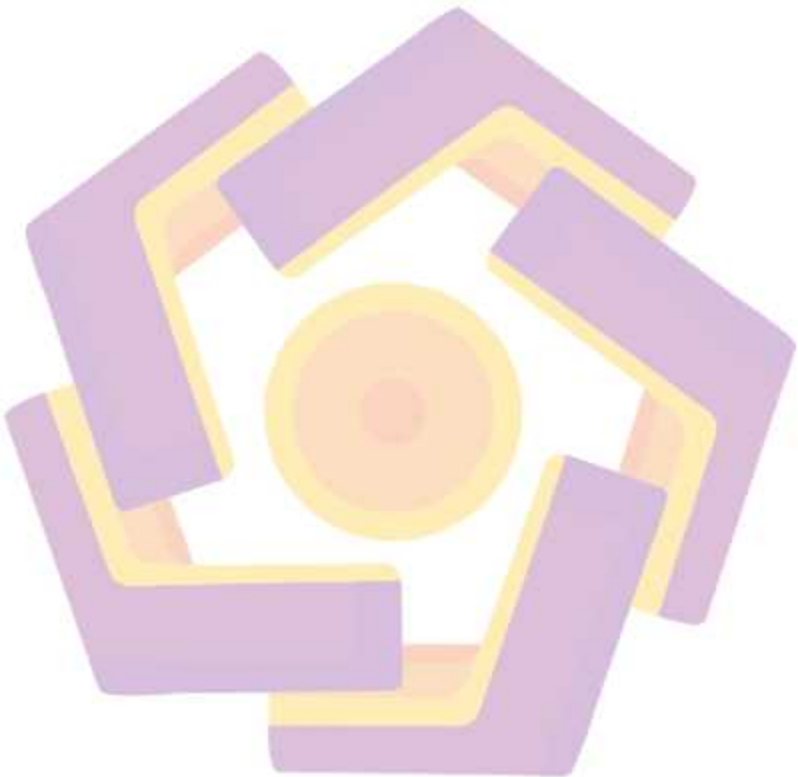
PT Sport Glove Indonesia merupakan perusahaan manufaktur yangmemproduksi sarung tangan yang beralamat di Krandon Pendowoharjo, Sleman, Yogyakarta. Perusahaan ini memiliki karakteristik make to order dalam proses produksinya. Perusahaan saat ini sudah mempunyai sistem jaringan komputer, namun belum ada sistemkeamanan untuk mengamankan sistem jaringan internal. Sedangkanperan jaringan dalam perusahaan sangat penting untukkomunikasidan penyimpanan data pekerjaan. Karena itu dibutuhkan suatu sistem untuk mendeteksi lalu lintas jaringan perusahaan.

Biasanya sistem keamanan yang dibangun pada sistem jaringan perusahaan hanya berfokus pada serangan external saja tanpa memperhatikan serangan dari dalam atau internal. Padahal serangan internal lebih berpotensi mengancam keamanan jaringan, Pasalnya karyawan yang berada dalam jaringan mempunyai akses langsung dengan kabel LAN dan dapat melihat secara langsung perangkat jaringan seperti router, switch, IP Address, sistem operasi, dan perangkat lain yang dapat dicari celah eksploitasinya.

Hasil survey Threat Report 2018 yang dipublikasikan Cyber Security Insiders menyebutkan bahwa sekitar 57% target serangan orang dalam atau internal perusahaan adalah informasi bisnis rahasia, termasuk keuangan, data pelanggan, dan data karyawan (14). Hal ini diperkuat oleh pernyataan dariSamore

Kuo (2018) yang menjelaskan bahwa "Jenis serangan orang dalam ini tidak terdeteksi selama





bertahun-tahun karena kesulitannya membedakan tindakan berbahaya dan pekerjaan rutin. Bahkan jika terdeteksi, karyawan dapat dengan mudah menyatakannya bahwa kesalahan terjadi secara tidak sengaja,"

Jaringan komputer pada PT. Sport Glove Indonesia mempunyai keamanan jaringan yang rendah, namun kegunaannya dalam aktivitas sangat krusial, sehingga peningkatan keamanan jaringan perlu dilakukan dengan perlahan-lahan dari hal yang paling dasar agar tidak mengganggu kinerja perusahaan.

Solusi yang dapat digunakan adalah dengan membangun sebuah *InstrusionDetection System* (IDS), IDS dapat membaca paket-paket yang masuk dan keluar dalam sebuah jaringan yang nantinya akan memberikan sebuah *log* kepada administrator jaringan. Dengan memanfaatkanIDS pada suatu jaringan makapaket paketyang berpotensi menjadi ancaman dapat tercatat pada *log* dan akan menjadi pertimbangan untuk pembuatan kebijakan sistem jaringan.

Snort adalah salah satu IDS yang bersifat *open source*.Snort beroperasi dengan berbasis *command line* dan telah diintegrasikan ke beberapa aplikasi pihak ketiga serta mendukung *cross platform*. Snort dapat menganalisis semua lalu lintas jaringan dan mengkategorikan jenis penyusupan dalam sebuah jaringan.

Dari uraian diatas maka dapat diambil penelitian dengan judul **"Implementasi Snort Sebagai Sistem Deteksi Intrusi Menggunakan CentOS 7.7.1908 pada PT. Sport Glove Indonesia."**

1.2 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk "Mengimplementasikan Snort IDS sebagai masukan kepada administrator jaringan untuk menentukan kebijakan sistem jaringan PT. Sport Glove Indonesia."

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, dapat dirumuskan sebuah permasalahan yaitu : "Bagaimanamengimplementasikan IDS sebagai bahan pengambilankebijakansistem jaringan pada PT. Sport Glove Indonesia?"

1.4 Batasan Masalah

Untuk mempersempit pembahasan pada tugas akhir ini, maka dibuat batasan-batasan sebagai berikut :

a. Server Snort IDS dibangun pada sistem operasi CentOS 7.7.1908
b. Menggunakan Snort IDS sebagai sistem pendeteksi intrusi
c. Implementasi Snort hanya dilakukan pada jaringan internal PT. SGI
d. Pengujian intrusi dilakukan dengan cara Port Scanning, Ping of Death, dan DoS
e. Jaringan yang digunakan menggunakan IPv4
f. Port pada jaringan menggunakan FastEthernet
g. Hasil IDS sebagai pengambilan keputusan kebijakan keamanan jaringan

1.5 Manfaat Penelitian

Manfaat penelitian yang dilakukan adalah :

1. Mampu mengimplementasikan Snort sebagai sistem deteksi intrusi pada jaringan

2. Mampu menjadi bahan pertimbangan kebijakan akses jaringan dari pihak yang tidak berhak mengaksesnya (*unauthorized user*)

1.6 Metodologi Penelitian

Metode penelitian yang akan penulis gunakan dalam penelitian ini adalahsebagai berikut :

1.6.1 Studi Pustaka

Tahap ini digunakan untuk mencari informasi yang berhubungan dengan permasalahan yang akan dibahas dengan bersumber pada buku-buku, serta bacaan lain yang dapat membantu menyelesesaikan penelitian.

1.6.2 Observasi

Tahap kedua ini digunakan untuk memperoleh data dengan cara melihat secara langsung kondisi obyek dan wawancara dengan Senior Asisten Manajer PT. Sport Glove Indonesia

1.6.3 Analisis

Data yang diperoleh dari hasil observasi dan wawancara yang telah dilakukan akan dianalisis untuk mengetahui pengembangan apa yang dapat diterapkan ke dalam sistem jaringan.

1.6.4 Pembuatan Sistem

Pada tahap ini kebutuhan sistem seperti perangkat keras dan perangkat lunak ditentukan sesuai dengan spesifikasi sistem yang diperlukan.

1.6.5 Implementasi

Setelah kebutuhan sistem tersedia, maka dilakukan implementasi penginstalan IDS beserta konfigurasinya. Hasil akhir dari tahap ini adalah IDS dapat berjalan pada sistem.

1.6.6 Pengujian

Pengujian dilakukan untuk membuktikan apakah sistem sudah berjalan dengan baik atau belum. Melalui pengujian IDS dengan Port Scanning, Ping of Death, dan DoS dapat diketahui performa IDS yang sedang dijalankan. Jika terjadi kesalahan maka perlu dikonfigurasi ulang sampai hasil yang diinginkan tercapai.

1.6.7 Sistematika Penulisan

Sistematika dalam penulisan tugas akhir ini dibagi menjadi lima bab, antara lain sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini berisi gambaran umum penulisan tugas akhir yaitu tentangLatar Belakang Masalah, Tujuan Penelitian, Rumusan Masalah, Batasan Masalah,danSistematika Penulisan.

BAB II TINJAUAN PUSTAKA

Berisikan tentang teori penunjang dan referensi-referensi berupa buku, jurnal, dan laporan tugas akhir sebagai acuan yang mendukungpenelitian.

BAB III TINJAUAN UMUM

Berisi penjelasan mengenai obyek penelitian, hasil observasi, masalah yang terdapat pada obyek, dan gambaran umum proyek.

BAB IV PEMBAHASAN

Bab ini menjelaskan tentang implementasi IDS, pengujian alat, dan evaluasi pengerjaan proyek.

.BAB V PENUTUP

Bab ini merupakan penutup dari penulisan tugas akhir. Terdapatkesimpulan dari penelitian yang dilakukan, sesuai dengan datadata yang sudah di olah. Dan terdapat juga saran dari penyelesaian Tugas Akhir ini yang berfungsibagi pengembang untuk melakukan Analisissi lebih mendalammengenai protokol yang dibahas.