BAB I

PENDAHULUAN

1.1. Latar Belakang

Internet merupakan salah satu penemuan terbesar bagi peradaban manusia. Informasi-informasi di seluruh belahan dunia bisa didapatkan dengan mudah tanpa bergerak sama sekali dari tempat kita berada. Internet telah menjadi gudang sumber informasi yang terus berkembang seiring dengan waktu. Fakta dan statistik memperlihatkan terjadinya sejumlah kecenderungan yang meningkat di dunia maya, misalnya jumlah pengguna dan pelanggan yang semakin bertambah, terbentuknya komunitas-komunitas dunia maya, dan sebagainya. Dan pada akhirnya, karena semakin banyaknya orang yang memanfaatkan internet, mengakibatkan "nilai" atau *"value"* dari dunia maya menjadi meningkat. Akibatnya, semakin banyak pihak yang merasa berkepentingan dengan keberadaan internet. Dari yang hanya ingin sekedar menjadi penyedia jasa pertukaran informasi hingga para kriminal yang memanfaatkan dunia maya untuk tujuan yang tidak baik. Sedikitnya terdapat isu-isu kejahatan internet yang sering muncul. Yaitu *virus/worm/trojan*, penetrasi sistem, serangan DoS/DDoS, *Spoofing*, sabotase jaringan, dan *unauthorized access*.

Teknologi firewall sebagai tembok penghalang dan *policy* dalam kejahatan internet dirasa tidak selalu efektif terhadap percobaan intrusi. Karena biasanya firewall dirancang untuk memblokir *traffic* di jaringan yang mencurigakan secara

tegas. Begitu juga dengan prosedur untuk mengizinkan paket untuk lewat jika sesuai dengan *policy* dari firewall. Masalahnya adalah banyak program *exploit* konsentrasi serangannya memanfaatkan firewall yang mengizinkan protokol tertentu untuk menembus firewall. Sebagai contoh, percobaan attacker untuk melakukan penetrasi melalui port 23 (telnet). Tetapi *policy* dari firewall memblokir permintaan untuk port 23. Mungkin attacker tidak bisa melakukan telnet ke komputer target karena *rule* dari firewall yang ketat. Tetapi firewall ternyata mengizinkan *request* (permintaan) dari luar untuk port 80 (http). Dan *attacker* dapat memanfaatkan port 80 untuk eksploitasi http. Ketika webserver telah berhasil dikuasai, firewall dapat dikatakan sudah di-*bypass* dan tidak berguna lagi.

Perkembangan keamanan internet menemukan gagasan baru. Dikembangkanlah *Intrusion Detection System* (IDS) sebagai sistem pintar yang bekerja dengan cara memantau *traffic* jaringan, menangkap dan memeriksa setiap paket yang lewat dalam jaringan, hingga mendeteksi adanya kejanggalan dalam jaringan berdasarkan *database signature* IDS, mungkin karena *traffic* padat/down atau karena adanya serangan. Kemudian IDS akan membuat *report* yang dapat dengan mudah dimengerti oleh *Network Administrator* untuk kemudian dilakukan tindak lanjut atas kejadian yang dilaporkan oleh IDS. Tetapi IDS adalah sistem yang pasif. IDS hanya memantau jaringan tanpa melakukan troubleshooting terhadap masalah yang terjadi. IDS pun tidak dapat melakukan pencegahan terhadap kejadian yang pernah terjadi sebelumnya. Untuk itu dilakukan pengembangan dari IDS. Perkembangan lanjut dari IDS adalah IPS (*Intrusion*

Prevention System). IPS diperkaya dengan kemampuan untuk melakukan pencegahan secara proaktif dalam jaringan terhadap gangguan yang sering atau pernah terjadi berdasarkan *signature* atau *anomaly* (statistik).

Perusahaan PT. Jamsostek merupakan program publik yang memberikan perlindungan bagi tenaga kerja untuk mengatasi resiko sosial ekonomi tertentu dan penyelenggaraannya menggunakan mekanisme asuransi sosial. Perusahaan ini adalah sebagai Badan Usaha Milik Negara (BUMN) yang dalam alur kerjanya terdapat banyak SDM yang berperan penting bagi laju berkembangnya perusahaan tersebut. Terdapat beberapa kendala pada PT. Jamsostek salah satunya adalah pengolahan keamanan jaringan pada PT. Jamsostek, banyaknya *attacker* yang menggunakan keahlian-keahliannya untuk bisa memasuki jaringan pada perusahaan tersebut agar bisa mendapatkan informasi atau data yang bersifat rahasia, untuk itu karyawan yang bertugas mengamankan jaringan komputer (*Network Administrator*) harus lebih waspada terhadap serangan-serangan yang dilakukan oleh penyusup. Untuk menangani serangan tersebut maka sudah menjadi tugas dari *Network Administrator* untuk mencegah serangan yang dilakukan oleh penyusup. Salah satu pencegahannya adalah menggunakan *Intrusion Prevention System* (IPS).

Demi efisiensi dan efektifitas kerja maka keamanan jaringan pada PT. Jamsostek sangat diperlukan. Dengan perkembangan bidang teknologi informasi yang semakin meningkat sudah saatnya kendala ini dapat diatasi. Maka akan dibutuhkan suatu sistem mengenai **"PERANCANGAN SISTEM PENCEGAHAN TERHADAP PENYUSUP MENGGUNAKAN SNORT**

DAN IPTABLES FIREWALL PADA PT. JAMSOSTEK (PERSERO) PUSAT".

1.2. Rumusan Masalah

Mengacu pada latar belakang yang telah dikemukakan diatas, maka penulis merumuskan masalah yang ada di PT. Jamsostek yaitu bagaimana merancang sebuah sistem pencegahan terhadap penyusup (Intrusion Prevention System) ?

1.3. Batasan Masalah

Dalam Penulisan tugas akhir penulis memberikan batasan agar masalahnya dapat terselesaikan dengan tepat sasaran, efektif, dan efisien. Pembahasan hanya masalah ruang lingkup analisa sistem pencegah penyerangan dari penyusup yang berusaha untuk merusak sistem jaringan yang dibagi menjadi beberapa bagian, yaitu :

1. Merancang *Intrusion Prevention System* (IPS) dengan menggunakan Linux CentOS, Snort dan blockit.
2. Memonitor jaringan dan / atau kegiatan yang tidak diinginkan sistem atau perilaku berbahaya dan dapat bereaksi secara *real-time*, untuk memblokir atau mencegah kegiatan tersebut.
3. Memantau semua lalu lintas jaringan untuk kode berbahaya atau serangan, Ketika ada serangan yang terdeteksi maka dapat di cegah,

sehingga memungkinkan semua lalu lintas data lainnya untuk lulus pencegahan.

1.4. Tujuan Penelitian

a. menganalisa dan Merancang suatu mekanisme untuk dapat Memonitor jaringan dan / atau kegiatan yang tidak diinginkan sistem atau perilaku berbahaya dan dapat bereaksi secara real-time, untuk memblokir atau mencegah kegiatan tersebut.

b. memberikan gambaran dan opini serta penjelasan kepada pihak yang berkepentingan untuk meningkatkan efektifitas kerja berdasarkan manfaat dari *Intrusion Prevention System* (IPS)

1.5. Metode Penelitian

Metode penelitian yang dilakukan penulis selama proses pembuatan tugas akhir adalah sebagai berikut :

1. Studi Pustaka

   Dilakukan dengan mempelajari buku-buku atau pustaka yang berhubungan dengan pokok pembahasan.

2. Studi Lapangan

   - Wawancara

Penulis melakukan wawancara dengan pihak terkait dalam kegiatan pengumpulan data.

- Observasi

  Teknik ini dilakukan untuk memperoleh data dengan melakukan pengamatan.

1.6. Sistem Penulisan

Sistematika penulisan tugas akhir ini terbagi kedalam lima bab beserta pokok materinya. Sebagai gambaran umum sistematika penyusunan tugas akhir yang akan ditulis adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai Latar Belakang Masalah, Identifikasi Permasalahan, Batasan Masalah, Maksud dan Tujuan, Metodologi Penelitian dan Sistematika Penulisan.

BAB II LANDASAN TEORI

Bab ini membahas mengenai landasan teori yang mendukung proses yang berhubungan dengan perancangan sistem pecegahan terhadap penyusup dengan menggunakan snort dan iptables firewall pada PT. JAMSOSTEK (PESERO)

BAB III ANALISA SISTEM YANG SEDANG BERJALAN

Bab ini menjelaskan tentang gambaran secara umum sistem yang berjalan dengan sistem yang akan dibuat dan menganalisa masalah yang berhubungan dengan sistem yang akan dibuat

BAB IV PERANCANGAN SISTEM

Dalam bab ini akan membahas mengenai perancangan dan pembangunan sistem yang diusulkan yang merupakan solusi dari permasalahan yang dihadapi.

BAB V KESIMPULAN DAN SARAN

Bab ini menguraikan kesimpulan dari penyelesaian masalah yang dibahas serta saran – saran yang diharapkan bermanfaat untuk pengembangan sistem.