BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan merupakan salah satu faktor penting dalam perkembangan teknologi dan informasi. Perkembangan jaringan tidak hanya sebagai media komukasi saja, namun jaringan adalah sebagai bagian dari kelangsungan hidup suatu individu, organisasi atau bisnis. Berbagai macam penggunaan jaringan mulai dari *social netwok*, pertukaran informasi, transaksi, dan juga penyimpanan data secara cloud server atau terpusat dalam suatu server. Jaringan yang menjadi sesuatu yang mutlak harus ada untuk memenuhi kebutuhan dalam pertukaran data dan kebutuhan informasi yang cepat.

Dalam mengembangankan jaringan selain dari segi perangkat keras yang tidak kalah penting adalah sebuah sistem kemanan jaringan yang melindungi dari segala macam serangan dan bentuk usaha-usaha penyusupan oleh pihak yang tidak berhak. keamanan jaringan adalah suatu bagian yang amat penting yang harus diperhatikan, Keamanan jaringan sebagai bagian dari sebuah sistem sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya.

Dengan semakin banyaknya cara untuk melakukan penyusupan kedalam jaringan internal untuk sekedar melakukan tes terhadap jaringan

tersebut seperti *scanning* atau pun membuat jaringan menjadi lumpuh dengan melancarkan *Denial of Service(DoS)* terlebih usaha untuk mendapatkan informasi penting dari server dan semakin banyak nya perangkat lunak yang beredar yang dapat gunakan untuk melakukan serangan serta penyusupan tentunya akan menyebabkan meningkatnya ancaman keamanan terhadap suatu jaringan. Hal ini tentunya sangat berbahaya terutama pada sektor-sektor yang memiliki tingkat keamanan data yang sensitif seperti objek – objek pemerintahan, perbankkan serta objek yang terhubung dengan sebuah jaringan. Untuk itulah diperlukan sebuah perhatian khusus dalam bidang keamanan jaringan yang bertujuan untuk mencegah terjadinya pencurian data dan arsip penting lainnya.

Dari data yang di unggah di situs http://www.arbornetworks.com/ 54% serangan sepanjang tahun ini lebih 1GB/detik naik dari 33% pada tahun 2012, 37% serangan sepanjang tahun ini antara 2-10 GB/detik naik dari 15% tahun lalu, pertumbuhan 44% dalam proporsi serangan lebih 10 Gb/detik sampai 4% dari semua serangan, untuk 2013 rata-rata serangan DDoS sekarang berdiri di 2.64 Gb/detik naik 78% dari 2012, 87% dari semua serangan dipantau sepanjang tahun ini berlangsung kurang dari satu jam ukuran serangan diverifikasi meningkat signifikan sampai 191 Gb/detik.

Untuk mengatasi masalah diatas perlu diterapkan suatu tindakan pengamanan jaringan yang dapat mendeteksi serangan dan mengamankan sistem. Kebanyakan dari sistem yang diterapkan biasanya

hanya berupa *IDS (Intrusion Detection System)* atau *IPS (Intrusion Prevention System)* yang mengakibatkan tidak maksimalnya tingkat keamanan jaringan pada suatu instansi yang hanya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Hal ini sangat berbahaya sehingga diperlukan sebuah sistem yang mampu menjadi *IDS* sekaligus menjadi *IPS* sehingga seorang administrator jaringan tidak harus memantau setiap kejadian yang berkaitan dengan adanya sebuah serangan.

Untuk itulah dikembangkan suatu sistem *IDPS (Intrusion Detection Prevention System)* sebuah sistem yang lebih efektif sehingga dapat digunakan tidak hanya sebagai sebuah *IDS* namun juga sekaligus sebagai *IPS*. Perancangan sistem ini akan memberikan suatu yang baru dalam melakukan penanganan terhadap keamanan jaringan yaitu membangun suatu *IDPS* yang mampu menangani kondisi jaringan.

Sistem *IDPS* akan mendeteksi penyusupan dengan metode signature-based menggunakan *IDS Snort* dan mengeluarkan alert untuk setiap tindakan penyusupan yang dikenali oleh *IDS Snort*. Selanjutnya *IPS* engine akan membaca alert yang telah di generate dan melakukan pemblokiran akses IP dari intruder berdasarkan informasi ip tersimpan pada alert yang di generate oleh *Snort IDS*.

Sistem ini sangatlah menarik untuk dikembangkan karena sistem yang berbasiskan *open source* ini memiliki fitur yang memudahkan

seseorang administrator jaringan untuk melakukan konfigurasi aturan-aturan yang akan diterapkan pada jaringan.

Permasalahan tersebut menjadi gagasan bagi penulis untuk menuangkannya kedalam penyusunan skripsi dengan mengambil judul " Perancangan Dan Implementasi deteksi intrusi dan sistem pencegahan (IDPS) di Server CentOS (Studi kasus : Yogya Crew/Indonesian Backtrack Reg. Yogyakarta) " . penelitian ini bertujuan membantu seorang administator dalam melakukan perancangan dan implementasi serta konfigurasi sistem IDPS di server CentOS. Sehingga dapat menciptakan sebuah sistem yang mampu meminimalisir serangan dan meningkatkan keamanan jaringan .

1.2 Rumusan Masalah

Melihat dari latar belakang masalah yang dituliskan di atas, maka permasalahan yang ada dapat dirumuskan sebagai berikut :

1. Bagaimana meminimalisir dan meningkatkan keamanan jaringan di server CentOS?
2. Bagaimana merancang sebuah sistem keamanan jaringan IDPS di server CentOS?
3. Bagaimana mengimplementasikan dan mengkonfigurasi sistem keamanan jaringan IDPS di server CentOS?

1.3 Batasan Masalah

Masalah yang diangkat dalam penulisan ini terlalu luas jika diteliti secara menyeluruh. Maka dari itu agar masalah tidak melebar kemana-mana penulis hanya meneliti:

1. Sistem IDPS akan mendeteksi penyusupan dengan metode signature-based menggunakan Snorby dan mengeluarkan alert untuk setiap tindakan penyusupan yang dikenali oleh Snorby Selanjutnya IPS engine menggunakan *Artillery* akan membaca alert yang telah di generate dan melakukan pemblokiran akses ip dari intruder berdasarkan informasi ip tersimpan pada alert yang di generate oleh Snorby.
2. Perangkat lunak yang di gunakan untuk sistem tersebut adalah *Snorby* yang di install di server CentOS dan kali linux sebagai penetrasi atau uji coba system IDPS.
3. Server Jogja Crew/Indonesian Backtrack Reg. Yogyakarta.

1.4 Tujuan Penelitian

Tujuan dari penulis mengambil judul " Perancangan Dan Implementasi deteksi intrusi dan sistem pencegahan (IDPS) di Server CentOS (Studi kasus : Yogya Crew/Indonesian Backtrack Reg. Yogyakarta) " ini adalah :

1. Sebagai salah satu syarat untuk menyelesaikan pendidikan program Strata 1 di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Dapat merancang dan mengimplementasikan sistem keamanan jaringan IDPS pada server CentOS.
3. Menghasilkan suatu sistem keamanan jaringan yang bisa digunakan dan dimanfaatkan oleh administrator.

1.5 Manfaat Penelitian

Manfaat yang diharapkan bisa diperoleh dari disusunnya skripsi ini adalah sebagai berikut:

1. Menghasilkan suatu sistem monitoring dan mampu mencegah serangan/gangguan dalam jaringan.
2. Suatu sistem yang dapat memberitahukan administrator jaringan tentang adanya gangguan keamanan pada jaringan.
3. Dapat membantu administrator untuk memelihara dan menerapakan kebijakan pada jaringan.
4. Dapat lebih memahami tentang aktifitas jaringan pada server CentOs.

1.6 Metode Penelitian

Dalam pembuatan judul " Perancangan Dan Implementasi deteksi intrusi dan sistem pencegahan (IDPS) di Server CentOS (Studi kasus :

Yogya Crew/Indonesian Backtrack Reg. Yogyakarta) " ini, penulis menggunakan metode sebagai berikut:

1. Requirement / eksplorasi kebutuhan pengguna
2. Analisis sistem
3. Design / perancangan
4. Implementasi
5. Pemeliharaan

Sedangkan untuk pengumpulan data, penulis menggunakan metode:

1. Metode Kepustakaan

   Merupakan metode yang dipakai untuk mendapatkan konsep-konsep teoritis melalui buku-buku sebagai bahan referensi dalam mendapatkan segala informasi yang dibutuhkan.

2. Metode Study Literatur

   Merupakan metode pengambilan data dengan menggunakan literatur yang ada, seperti dengan mengunjungi situs-situs web yang memiliki hubungan dengan permasalahan yang diambil, yaitu memanfaatkan fasilitas internet.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penyusunan skripsi disesuaikan dengan ketentuan lembaga, yaitu sebagai berikut:

BAB I PENDAHULUAN

Bab ini meliputi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta sistematika penulisan yang dipakai dalam menyusun skripsi.

BAB II LANDASAN TEORI

Bab ini menjabarkan teori-teori dalam berbagai askpek yang mendasari pembahasan secara detail, berupa definisi-definisi ataupun model matematis yang berkaitan dengan system IDPS.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjabarkan tinjauan umum analisis sistem, analisis kebutuhan sistem, perancangan sistem secara umum, dan perancangan sistem.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini akan memaparkan hasil program dari tahap penelitian lebih lanjut mengenai implementasi sistem IDPS, dan pembahasan hasil pengujian sistem IDPS dengan hasil output.

BAB V PENUTUP

Bab ini merupakan bab terakhir dari sistematika penulisan skripsi. Di dalam bab ini memuat kesimpulan serta saran dari sistem.