BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dewasa ini perkembangan dalam bidang teknologi dan informasi semakin pesat, ini terbukti dengan semakin banyaknya manusia menggunakan layanan jaringan internet pada komputer. Seiring dengan perkembangan jaringan internet yang sedemikian pesat menjadikan keamanan suatu data atau informasi menjadi sangatlah penting. Data yang cukup mengejutkan baru saja digelontorkan Akamai Technologies. Di situ tertulis bahwa Indonesia menempati urutan teratas sumber serangan cyber di seluruh dunia. Berdasarkan laporan keamanan tersebut, Indonesia mengantongi porsi terbesar serangan dengan perolehan 38%, naik 17% dari periode sebelumnya. Sedangkan China, yang sebelumnya mendominasi, kini hanya memiliki porsi 33%. Menurutnya, ada beberapa hal yang jadi pemicu Indonesia sebagai sarang serangan cyber. Salah satunya kontrol keamanan internet yang kurang ketat dari pemerintah dan kurangnya kepedulian para pihak penggelola IP di Tanah Air [**1**]. Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. [**2**]

Untuk dapat mengatasi permasalahan tersebut digunakan *Intrusion Detection System* (IDS) untuk mencegah serangan yang akan masuk ke jaringan komputer. IDS yang digunakan akan dipasangkan sebelum masuk kepada firewall pada komputer, sehingga akan muncul alert terlebih dahulu untuk menandakan bahwa ada sebuah aktifitas yang mencurigakan pada paket data yang akan masuk pada jaringan komputer. *Intrusion Detection System* (IDS) akan mencatat (*log*) semua paket data yang lewat secara mendetail. Lebih khusus, *Intrusion Detection System* (IDS) dapat mengirimkan *alert* dengan cara mengirimkan *e-mail* kepada *network administrator*. [**3**]

Dari masalah-masalah diatas maka akan dilakukan penelitian mengenai **"Implementasi Sistem Keamanan Data Menggunakan Metode *Intrusion***

Detection System **(IDS) Pada Protokol Jaringan IPv4 Dan IPv6"** sebagai salah satu metode sistem keamanan jaringan, hasil dari penelitian berupa analisa penggunaan sistem keamanan IDS pada protokol jaringan IPv4 dan IPv6.

1.2 Rumusan Masalah

Sistem keamanan komputer sangat penting diterapkan dalam sebuah jaringan komputer, karena akan berhubungan dengan berbagai macam aspek yang cakupannya luas. *Intrusion detection system* dapat dijadikan salah satu sistem keamanan untuk mendeteksi penyusup pada protokol jaringan IPv4 dan IPv6. Maka dari uraian diatas dapat didefenisikan permasalahannya antara lain:

1. Bagaimana penerapan sistem keamanan pada protokol jaringan IPv4 dan IPv6
2. Bagaimana administrator dapat mengetahui apabila jaringan pada IPv4 dan IPv6 sedang diserang.
3. Bagaimana *intrusion detection system* bekerja dengan menggunakan metode signatured based.
4. Bagaimana *Intrusion detection system* mampu memberikan peringatan jika terjadi sebuah ancaman.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah untuk mengimplementasikan sistem keamanan data pada jaringan dengan menggunakan *Intrusion Detection System* (IDS) pada mekanisme perubahan protokol jaringan IPv4 dan IPv6 dalam mendeteksi penyusup yang dapat merusak sistem. Sedangkan tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Menerapkan sistem yang secara aktif dalam memonitoring segala ancaman pada sistem jaringan

2. Mempermudah administrator dalam mendeteksi melihat history log dari serangan atau ancaman yang terjadi didalam sistem jaringan sehingga dapat melakukan sebuah tindakan lebih lanjut.
3. Memberikan penjelasan dan analisa mengenai *intrusion detection system* khususnya dengan menggunakan metode signatured based
4. Manampilkan hasil dengan *alert* terhadap terjadinya serangan dengan dalam bentuk GUI (*Grafik User Interface*)

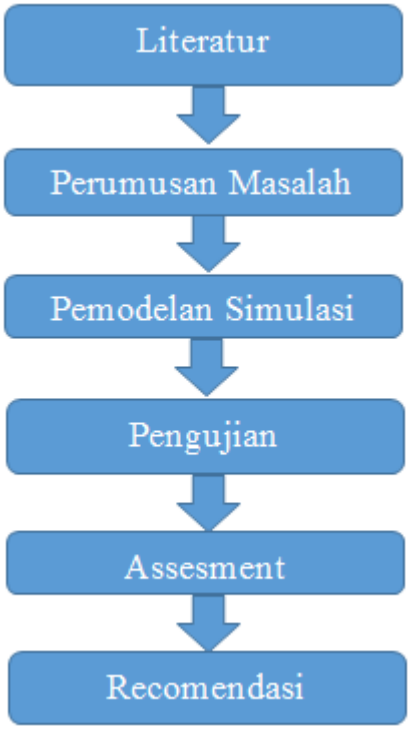
1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Menggunakan protokol jaringan IPv4 dan IPv6
2. Mengkonfiurasi sistem keamanan IDS dengan menggunakan aplikasi *snort* yang memiliki fungsi untuk melakukan pendeteksian terhadap serangan dan *alerting*.
3. Melakukan percobaan penyerangan menggunakan *Port Scanning* dan *ping of death*
4. Laporan Module yang digunakan untuk mengelola data-data peringatan (alerting) yang dihasilkan oleh SNORT dan menampilkan dalam bentuk tampilan Web GUI (Grafic User Interface) dengan menggunakan BASE (*Basic Analysis Security Engine*).
5. Hasil daari penelitian berupa rule-rule untuk jenis serangan *Port Scanning* dan *Ping of death*

1.5 Metodologi Penelitian

Metodologi yang digunakan pada penelitian tugas akhir ini yaitu dengan melalui tahap pengumpulan data. Adapun metode pengumpulan data yang dilakukan adalah sebagai berikut:



Gambar 1.1 Metodologi Penelitian

1. Literatur

   Studi literatur dilakukan dengan cara membaca dan mengkaji sumber buku, jurnal, maupun *paper* serta bacaan lainnya yang sesuai dan terkait dengan masalah yang sedang diteliti. Hingga saat ini, kajian tentang keamanan jaringan menggunakan metode *intrusion Detection System (IDS)* pada IPv4 dan IPv6 masih jarang ditemukan dalam penjelasan berbahasa Indonesia, sehingga studi literatur yang dilakukan lebih banyak mengacu pada *textbook* serta website resmi yang berkaitan.

2. Perumusan masalah

   Melakukan analisa terhadap masalah-masalah yang biasanya muncul terhadap jaringan komputer, analisa dilakukan dengan menganalisa beberapa artikel, jurnal, paper serta hasil survey

3. Pemodelan dan Simulasi

   Membuat model simulasi dalam hal ini adalah arsitektur jaringan yang digunakan untuk menganalisa jenis serangan dan menganalisa mengenai cara kerja dari *intrusion detection system.*

4. Pengujian

   Pengujian dilakukan dengan menerapkan *intrusion detection system* dengan menggunakan aplikasi snort dan aplikasi penunjang lainnya pada sebuah komputer yang akan dijadikan *server*. Proses pengujian dilakukan dengan menyerang ke *server* tersebut dengna beberapa metode penyerangan yaitu port scanning dan *Ping of death.* Adapun parameter sebagai tolak ukur pengujian yaitu:

   a. Ketepatan dalam pendeteksian serangan
   b. Terpantaunya aktifitas serangan pada server dengan adanya alert

5. Assesment

   Pada tahap *assesment, attacker* yang terkoneksi dengan *server* akan mengakses layanan pada *server* dan kemudian melakukan serangan dengan metode *port scanning, ping of the death* dll.

6. Rekomendasi

   Merekomendais pencegahan terhadap serangan-serangan yang mungkin terjadi pada *server* khususnya *port scanning* dan *ping of the death.*

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini bertujuan untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan ini diatur dalam lima bab:

BAB I PENDAHULUAN

Bab ini memaparkan tentang latar belakang masalah, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang berbagai konsep dasar dan teori-teori yang berkaitan dengan jaringan, protokol jaringan IPv4, protokol jaringan IPv6, metode *Dual Stack*, keamanan jaringan, serta *intrusion detection system*, dan lain-lain

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi pemaparan analisis masalah, analisis sistem operasi, analisis sistem yang sedang berjalan, analisis kebutuhan data, analisis jaringan, jaringan komputer, analisis kebutuhan sistem. Hasil dari analisis tersebut digunakan untuk melakukan perancangan arsitektur jaringan dan perancangan rule IDS.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini menjelaskan implementasi *Intrusion detection system* khususnya aplikasi snort pada protokol jaringan IPv4 dan IPv6, dijelaskan mengenai konfigurasi perangkat dan instalasi perankat lunak yang dibutuhkan. Pada bab ini juga dijelaskan pemaparan dari proses translasi dari tahap analisis dan perancangan ke tahap konfigurasi sehingga terbentuk sistem yang susai dengan hasil analisis dan perancanan.

BAB V KESIMPULAN DAN SARAN

Pada bab ini akan dibahas mengenai kesimpulan dari keseluruhan masalah yang telah dibahas pada bab sebelumnya dan dilengkapi dengan saran-saran yang dapat dijadikan masukan untuk kemudian dapat dikembangkan dan disempurnakan dimasa yang akan datang.