

BAB 1

PENDAHULUAN

Dalam bab ini membahas mengenai pendahuluan dari tugas akhir meliputi latar belakang, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi tugas akhir dan sistematika penulisan tugas akhir

1.1 Latar Belakang

Keamanan sudah menjadi hal yang penting dalam dunia teknologi informasi dan internet sudah menjadi kebutuhan dasar. Saat ini internet mempengaruhi hampir semua aspek kehidupan. Internet banyak memuat informasi dan layanan bagi para penggunanya seperti *web*, *cloud storage*, *file server* termasuk unggah dan unduh *file*, serta hiburan seperti sosial media dan *game online*.

Sistem yang paling umum digunakan pada internet adalah *client-server*. Server bertanggung jawab menyediakan, memelihara dan menjaga layanan tersebut sehingga dapat digunakan oleh *client* atau pengguna sebagaimana mestinya. Namun ada pihak tertentu yang sengaja menyerang server dengan motif, tujuan dan cara yang berbeda. Salah satu metode penyerangan tersebut adalah DDoS (Distributed Denial of Service). DDoS mampu membuat server menjadi sibuk dengan banyaknya permintaan layanan. Akibatnya server menjadi *hang*, *reboot* bahkan *crash*. Dampaknya layanan yang seharusnya diberikan kepada pengguna terganggu bahkan sama sekali tidak bisa digunakan. [MAR14]

PKP2A I LAN (Lembaga Administrasi Negara) merupakan salah satu aparatur negara kajian dan inovasi di bidang administrasi negara yang menyelenggarakan pendidikan dan pelatihan aparatur yang didalamnya memanfaatkan jaringan komputer untuk berjalanya proses bisnis seperti pengelolaan data online. Diantaranya untuk mengelola data pegawai, sistem absensi, data pendidikan dan pelatihan aparatur, dll. Dari hasil observasi dan wawancara dengan admin jaringan PKP2A I LAN didapatkan celah keamanan yang sangat riskan akan ancaman serangan ke jaringan PKP2A I LAN seperti, *Ping of Death*, *DoS* dll. Oleh sebab itu diperlukan sebuah metode pendeteksian keamanan yang baik seperti *firewall*, *ids* lain sebagainya.

Dari hasil observasi yang penulis lakukan di pkp2A I LAN pada system yang berjalan saat ini sering terjadi serangan DDoS yang mengakibatkan berhentinya proses bisnis sehingga dibutuhkan mesin pendeteksi untuk meminimalisir resiko dari server overload yang mengakibatkan aktivitas proses bisnis berhenti.

Berdasarkan masalah di atas, IDS menjadi solusi yang diterapkan pada tugas akhir ini. IDS merupakan singkatan dari *Intrusion Detection System*, yaitu sistem yang mampu menganalisis, mendeteksi jika terjadi tindakan mencurigakan dan serangan terhadap server. IDS yang digunakan adalah Suricata. Suricata bekerja berdasarkan *rule* atau aturan yang dibuat. Oleh

karena itu, implementasi sistem pencegahan DDoS menggunakan Suricata ini diharapkan mampu menjaga layanan yang diberikan server terhadap pengguna.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah di paparkan terdapat beberapa masalah yang timbul dalam sistem keamanan jaringan, yaitu :

1. Server rawan terhadap serangan DDoS dan tidak mempunyai pendeteksian serangan DDoS.
2. Dibutuhkan sebuah *System* yang mampu mencegah dan menangani serangan DDoS terhadap server

1.3 Tujuan Tugas Akhir

Adapun Maksud dan Tujuan dari tugas akhir ini adalah :

Membuat atau merancang dan memberikan peringatan kepada *admin* jika ada serangan DDoS terhadap web site bandung.lan.go.id

1.4 Lingkup Tugas Akhir

Adapun lingkup Tugas Akhir ini antara lain :

1. Implementasi Suricata menggunakan VMware
2. Menjelaskan cara kerja dan jenis serangan DDoS
3. Menjelaskan cara kerja IDS
4. Hanya melakukan uji coba serangan DDoS dengan jenis *Ping Of Death, Syn Attack, Scanning*
5. Hanya melakukan pendeteksian serangan DDoS menggunakan IDS
6. Tidak ada upaya pengamanan *database*
7. Tidak menggunakan *router*
8. Mesin IDS yang digunakan suricata di install di VMware

1.5 Metodologi Tugas Akhir

Metodologi Dalam Penelitian Tugas Akhir ini yang digunakan antara lain:

1. Studi Literatur / Studi Pustaka

Mempelajari hal yang berkaitan dengan Tugas Akhir, seperti IDS, DDoS dan Suricata. pengumpulan data yang dilakukan dengan mencari dan mempelajari berbagai data dari berbagai sumber seperti buku, modul, artikel, paper dari internet yang berkaitan dengan topik *Intrusion Detection System*.

2. Wawancara

Melakukan tanya jawab dengan ahli dibidang keamanan jaringan atau admin jaringan

3. Observasi

Observasi merupakan suatu metode pengumpulan data yang dilakukan dengan cara mengamati kejadian yang sedang berlangsung dilapangan.

4. Analisis

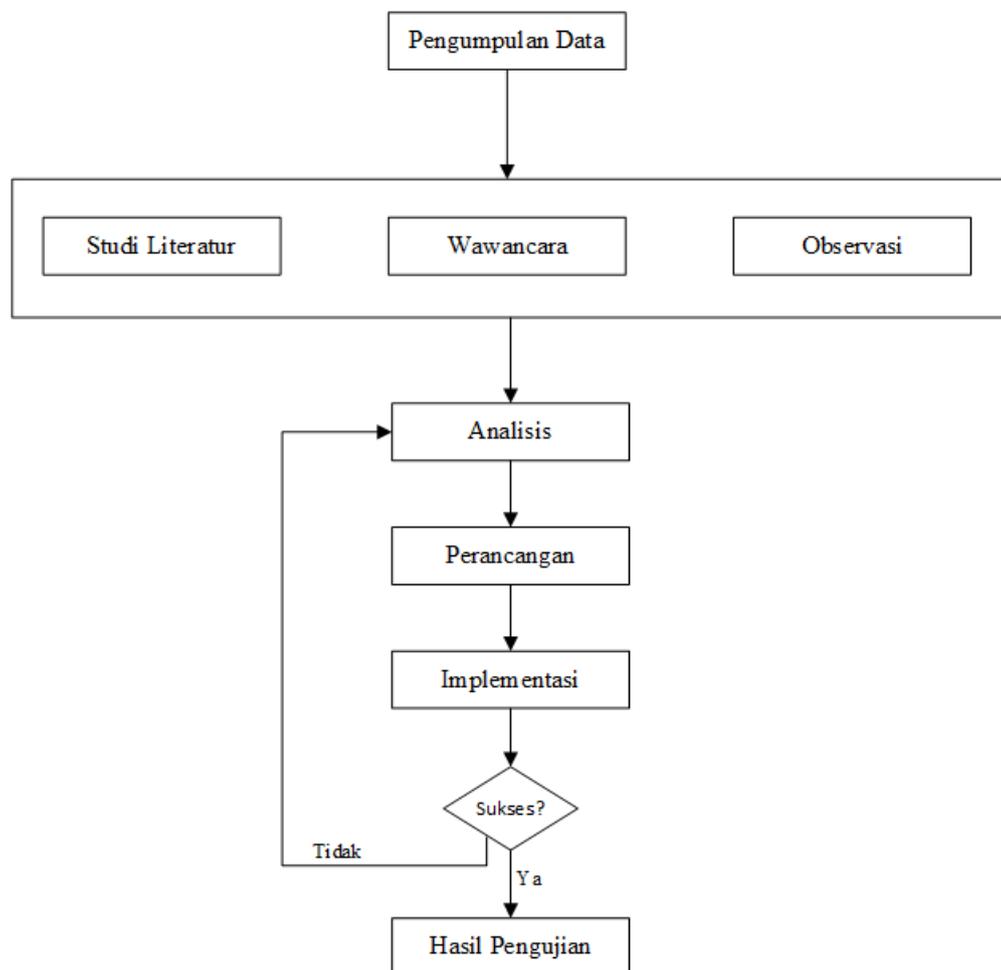
Analisis dilakukan untuk menjawab rumusan masalah dan untuk mengelola data lapangan sehingga menjadi bahan penelitian untuk tahap selanjutnya.

5. Perancangan Dan Implementasi sistem

Implementasi memuat hal mengenai instalasi dan konfigurasi semua aplikasi yang dibutuhkan.

6. Ujicoba Dan Evaluasi Sistem

Pengujian dilakukan setelah instalasi dan konfigurasi berjalan dengan baik, berupa simulasi serangan DDoS terhadap kemampuan suricata untuk kemudian menganalisis hasilnya.



Gambar 1-1 Metodologi Tugas Akhir

1.6 Sistematika Penulisan

Sistematika Penulisan Laporan Tugas Akhir ini terdiri dari beberapa Bab antara lain :

BAB 1 PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, rumusan masalah, lingkup tugas akhir, tujuan tugas akhir langkah – langkah pengerjaan tugas akhir dan sistematika penulisan laporan tugas akhir.

BAB 2 LANDASAN TEORI

Bab ini membahas definisi- definisi dan konsep-konsep dasar yang digunakan dalam penelitian tugas akhir ini, meliputi pembahasan tentang Keamanan jaringan, *IPS (Intrusion Detection System)*, *Tools* yang digunakan dalam penelitian ini.

BAB 3 SKEMA PENELITIAN

Bab ini membahas tentang analisis yang dilakukan untuk menjawab rumusan masalah dan membuktikan hipotesis dari rumusan masalah yang telah dilakukan.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi penerapan sistem yang telah dirancang sebelumnya dan diimplementasikan di jaringan,

BAB 5 KESIMPULAN DAN SARAN

Bab ini membahas tentang kesimpulan dan saran berdasarkan penyusunan laporan tugas akhir ini.

DAFTAR PUSTAKA

Daftar pustaka berisi tentang sumber-sumber yang digunakan dalam penyusunan tugas akhir.