BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan pada jaringan merupakan hal yang sangat penting, terutama kaitanya untuk menjaga validitas dan integritas data, serta untuk menjamin ketersediaan layanan bagi penggunanya. Oleh karena itu dibutuhkan sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat dan memungkinkan administrator sistem mengakses sistem walaupun terjadi malfungsi jaringan. Intrusion Detection System (IDS) adalah suatu perangkat lunak (software) atau suatu sistem perangkat keras (hardware) yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan dapat menganalisis keamanan jaringan [1].

Monitoring keamanan jaringan diperlukan dengan tujuan memberikan peringatan adanya penyusupan terhadap sistem. Sehingga dampak negatif yang ditimbulkan dapat diminimalisir baik pada penyedia layanan maupun pada pengguna. Belum adanya sistem monitoring jaringan pada Dinas Sosial Kabupaten Gunungkidul membuat permasalahan yang ada pada *server* layanan seperti FTP *server* menjadi lambat untuk ditangani. Terutama kaitannya dengan adanya serangan atau intrusi yang menyebabkan kerentanan pada bocornya data atau informasi yang ada. Sehingga akan menimbulkan masalah dikemudian hari yang dapat berakibat mengganggu atau menghambat kinerja dari karyawan di Dinas Sosial Kabupaten Gunungkidul. Oleh karena itu dibutuhkan sistem monitoring jaringan yang akan memberikan peringatan kepada administrator jaringan saat

adanya tindakan penyerangan atau penyusupan pada jaringan. Sehingga administrator jaringan dapat dengan cepat mengambil tindakan yang diperluhkan.

Salah satu perangkat lunak yang digunakan sebagai IDS adalah Snort. Snort merupakan suatu perangkat lunak untuk mendeteksi penyusupan yang mampu menganalisis paket yang melintasi jaringan secara *real time traffic* dan *logging* ke dalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan [1]. Hasil deteksi berupa *log* yang tersimpan dalam database akan dihubungkan dengan aplikasi *instant messaging*. Aplikasi inilah yang akan membantu andministrator jaringan untuk memberikan peringatan adanya tindakan penyusupan yang terjadi.

Aplikasi *instant* messaging yang populer dan banyak digunakan salah satunya adalah Telegram. Telegram memiliki fitur *chat* yang dapat digunakan untuk memberikan notifikasi singkat dengan cepat. Selain itu fitur pertukaran dokumen yang ada, dapat dimanfaatkan untuk memberikan rekap laporan penyusupan atau serangan pada sistem dalam jangka waktu tertentu dalam bentuk *file* dokumen.

Sistem peringatan (*alert*) yang dibuat ini akan memberikan peringatan kepada administrator jaringan dalam bentuk notifikasi singkat pada sistem yang sudah dipasangi IDS, jika terdeteksi adanya aktifitas serangan atau penyusupan. Notifikasi juga akan diberikan dalam bentuk *file* dokumen yang akan dikirimkan dalam jangka waktu tertentu. Selain itu aktifitas serangan atau penyusupan yang telah terdeteksi dapat dilihat dan dianalisa dengan lebih *detail* melalui tampilan antarmuka website. Serta tindakan pencegahan yang diperluhkan seperti blok

serangan berdasarkan IP address dapat dilakukan melalui antarmuka website tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah sebagai berikut :

Bagaimana memanfaatkan aplikasi *instant messaging* yaitu Telegram untuk dapat memberikan notifikasi adanya penyusupan atau serangan yang terjadi pada jaringan ?

1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Server yang dilindungi yaitu sebuah *server* Ubuntu 16.04 LTS yang memiliki layanan FTP, SSH, dan Web Server.
2. Notifikasi dikirim melalui aplikasi *instant messaging* Telegram.
3. Pengujian sistem yang dilakukan berupa *Port Scanning*, FTP *Bad login*, SSH Akses, Ddos *Attack*.
4. Metode pengembangan pada penelitian ini menggunakan NDLC (*Network Development Life Cycle*) namun hanya sampai pada tahap *monitoring*.
5. Server IDS dibangun dalam bentuk *prototype*, dan kemudian dilakukan implementasi dan pengujian langsung pada topologi jaringan Dinas Sosial Kabupaten Gunungkidul.

1.4 Maksud dan Tujuan Penelitian

Maksud dari penelitian ini adalah :

1. Membangun sistem yang dapat membantu administrator jaringan dalam mengurangi resiko keamanan yang terus meningkat.

Sementara tujuan dari penelitian ini adalah :

1. Merancang sistem yang dapat memberikan peringatan dini (*alert*) melalui notifikai *instant messaging* Telegram kepada administrator jaringan dalam menunjang penentuaan tindakan pengamanan jaringan.
2. Membangun sistem yang dapat memberikan peringatan dini (*alert*) melalui notifikai *instant messaging* Telegram kepada administrator jaringan dalam menunjang penentuaan tindakan pengamanan jaringan.
3. Membangun sistem yang dapat mendeteksi adanya serangan berupa *Ddos Attack, Port Scanning, SSH Akses,* dan *FTP Bad Login.*

1.5 Metode Penelitian

1.5.1 Pengumpulan Data

Metode penelitian yang digunakan untuk menadapatkan informasi tentang permasalahan penelitaian adalah :

1.5.1.1 Metode Studi Referensi

Studi referensi merupakan metode pengumpulan data dengan membaca berbagai referensi atau literatur yang mengacu dengan pembuatan sistem. Adapaun referensi – referensi tersebut adalah jurnal ilmiah nasional, dan buku koleksi perpustakaan Universitas AMIKOM Yogyakarta dan *file* dari internet. Data yang

didapatkan dengan metode ini nantinya digunakan sebagai referensi dalam melakukan penelitian.

1.5.1.2 *Interview* (Wawancara)

Metode wawancara dipakai untuk mengumpulkan data primer dari lingkungan internal organisasi maupun eksternal organisasi. Narasumber yang diwawancarai merupakan orang yang relevan dan berkaitan dengan data yang ingin didapatkan. Pada penelitian ini narasumber yang diwawancarai adalah administrator jaringan Dinas Sosial Kabupaten Gunungkidul. Metode ini untuk mendapatkan data topologi jaringan yang digunakan dan kemanan jaringan yang sudah diterapkan.

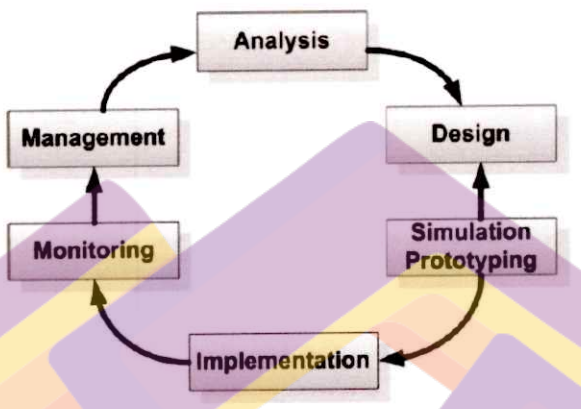
1.5.1.3 Observasi

Teknik pengamatan menurut Sugiono (2013) mengemukakan bahwa observasi merupakan salah satu proses yang kompleks, suatu proses yang tersusun dari berbagai proses biologis dan psikologis [2]. Dalam penelitian ini metode observasi atau pengamatan langsung digunakan untuk pengumpulan data dan fakta yang efektif untuk mempelajari suatu jaringan komputer. Kegiatan pada metode ini dilakukan dengan melakukan pengamatan langsung terhadap kegiatan yang sedang berjalan.

1.5.2 Metode Pengembangan

Metode pengembangan yang digunakan penulis dalam penelitian adalah NDLC (*Network Development Life Cycle*). NDLC merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya, seperti perencanaan strategi

bisnis, daur hidup pengembangan aplikasi, dan analisa pendistribusian data.. Adapun tahapan pada NDLC terdapat pada Gambar 1.1.



Gambar 1.1 ***Network Development Life Cycle*** **[3]**

NDLC memiliki enam tahap dalam strategi pengembangannya, yaitu *Analysis* (Analisa), *Design* (Perancangan), *Simulation Prototyping* (Simualasi Prototipe), *Implementation* (Penerapan), *Monitoring* (Pemantauan), dan *Management* (Pengelolaan).

Pada metode pengembangan ini menjelaskan tahapan – tahapan pada penelitian, mulai dari tahap awal hingga tahap akhir. Terdapat lima tahapan utama yang dilakukan dalam penelitian yaitu tahap *Analysis* (Analisa), tahap *Design* (Perancangan), tahap *Simulation Prototyping* (Simualasi Prototipe), tahap *Implementation* (Penerapan), dan tahap *Monitoring* (Pemantauan). Berdasarkan batasan masalah yang telah ditentukan, penggunaan metode NDLC hanya digunakan sampai tahap *monitoring*. Penjelasan dari setiap tahapan adalah sebagai berikut :

1.5.2.1 *Analysis* (Analisa)

Pada bagian *analysis* atau analisa dilakukan proses penelitian awal terdiri dari analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan *user*, dan analisa topologi jaringan saat ini.

1.5.2.2 *Design* (Perancangan)

Tahap selanjutnya adalah desain atau perancangan dalam tahap pembangunan yang akan diimplementasikan, perancangan sistem IDS meliputi hubungan antar modul dalam sistem, serta alur kerja IDS Server.

1.5.2.3 *Simulation Prototyping* (Simualasi Prototipe)

Tahap selanjutnya adalah membuat prototipe menggunakan *virtualbox* dengan menerapkan topologi yang dibuat pada tahap sebelumnya.

1.5.2.4 *Implementation* (Penerapan)

Pada tahapan implementasi ini akan diterapkan apa yang telah direncanakan dengan dilakukannya pembuatan *prototyping* terhadap desain infrastruktur. Dalam tahap ini mencangkup instalasi serta konfigurasi sistem terhadap desain topologi jaringan yang telah direncanakan serta melakukan pengujian terhadap sistem.

1.5.2.5 *Monitoring* (Pemantauan)

Tahap *monitoring* merupakan tahapan yang menjamin agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal pada tahap analisa. *Monitoring* dilakukan terhadap performa sistem IDS yang meliputi kemampuan deteksi, akurasi, dan kecepatan.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini terdiri dari dari lima bab yang terdiri dari :

1. BAB I : PEDAHULUAN

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

2. BAB II : LANDASAN TEORI

   Bab ini akan menguraikan tinjauan pustaka dan dasar – dasar teori yang berkaitan dengan skripsi atau tema yang sama dengan penelitian ini.

3. BAB III : ANALISIS DAN PERANCANGAN

   Bab ini akan membahas mengenai analisis sistem dan perancangan yang akan digunakan dalam pembuatan sistem, alat – alat yang digunakan serta sistematika pengujian yang akan dilakukan.

4. BAB IV : IMPLEMENTASI DAN PEMBAHASAN

   Bab ini membahas tentang instalasi dan konfigurasi sistem dalam jaringan, hasil uji serta perbedaan kondisi sebelum dan sesudah implementasi *Intrusion Detection System* dengan Snort.

5. BAB V : PENUTUP

   Bab ini menyampaikan kesimpulan dari rumusan masalah dan menyampaikan saran tentang pengembangan sistem yang telah dibuat serta untuk pengembangan selanjutnya.