BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi khususnya jaringan komputer, saat ini sudah berkembang semakin cepat. Perkembangan teknologi ini memudahkan para pengguna untuk melakukan berbagai pekerjaan, seperti bertukar informasi, mencari data, juga sebagai media penghubung antara seseorang dan yang lainnya. Di satu sisi, perkembangan jaringan komputer khususnya internet memberikan dampak yang sangat baik untuk penggunanya, namun di sisi lain juga memunculkan beberapa permasalahan yang cukup serius, salah satunya yaitu faktor keamanan.

Keamanan jaringan merupakan isu yang sangat penting, seiring dengan pentingnya informasi yang terkandung pada sebuah jaringan maka dibutuhkan sistem keamanan jaringan untuk mengamankan data ataupun memantau aktifitas mencurigakan yang ada pada sebuah jaringan. IDS akan memonitor lalu lintas data pada sebuah jaringan dan akan menganalisa dengan algoritma tertentu yang akan memutuskan memberi peringatan kepada seorang administrator jaringan apakah ada aktivitas mencurigakan atau tidak.

Bagi sebuah instansi maupun golongan tertentu, keamanan jaringan merupakan salah satu proses untuk mencegah serta mengantisipasi resiko terjadinya berbagai ancaman yang mungkin dapat terjadi sehingga dapat merusak sistem kinerja jaringan. SMA Negeri 11 Yogyakartta merupakan salah satu instansi yang menggunakan jaringan komputer di laboratorium jaringannya. Saat ini laboratorium tersebut belum memiliki sistem untuk memonitoring jaringan

dan yang bertanggung jawab terhadap semua jenis keamanan pada laboratorium tersebut adalah administrator. Laboratorium SMA Negeri 11 dalam kurun waktu bulan Mei 2018 mengalami 4 serangan dari dalam pada saat praktikum oleh siswa iseng yang mengakibatkan ada komputer saat itu tidak dapat mengakses internet karena pelaku merubah informasi konfigurasi seperti merubah *routing* (perjalanan) informasi ke dalam router, sehingga jaringan korban tidak dapat berfungsi. Serangan yang dilakukan berupa DDOS *Attack*.

Tugas seorang administrator cukup berat, karena administrator harus selalu memantau dan melaporkan keadaan jaringannya jika terjadi gangguan atau penyusupan. Sistem pelaporan keamanan terhadap aktifitas-aktifitas dalam jaringan yang ada saat ini masih dilakukan secara manual oleh administrator. Oleh sebab itu, dibutuhkan suatu sistem keamanan yang berfungsi untuk membantu administrator dalam memonitoring jaringan.

Untuk mengatasi permasalahan yang ada, perlu dibangun sebuah sistem yang memonitor keamanan jaringan secara *realtime*. Dalam penelitian ini, penulis akan merancang suatu sistem yang berguna untuk memonitor gangguan-gangguan pada jaringan menggunakan Snort dan mengirimkan notifikasi gangguan yang terekam oleh Snort melalui Telegram pada *handphone* / komputer administrator jaringan sebagaimana kasus yang terjadi pada laboratorium SMA Negeri 11 Yogyakarta, agar membantu pekerjaan administrator dalam memonitor kondisi jaringannya. Dengan demikian, administrator akan memperoleh pesan notifikasi secara langsung yang memuat informasi mengenai kondisi atau gangguan jaringan yang dikelolanya.

1.2 Rumusan Masalah

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

1. Bagaimana membuat sistem yang berfungsi untuk memonitoring keamanan jaringan dan mengirimkan notifikasi kepada administrator ketika terjadi gangguan pada jaringan tersebut?
2. Bagaimana pengaruh penerapan NIDS dari sisi keamanan jaringan di SMA Negeri 11 Yogyakarta ?

1.3 Batasan Masalah

Berdasarkan penelitian yang akan dilakukan penulis, maka penulis menjabarkan batasan-batasan penelitian sebagai berikut :

1. Sistem ini ditujukan pada SMA Negeri 11 Yogyakarta.
2. *Intrusion Detection System* yang digunakan adalah *Snort v2.9.11.1*
3. Jenis konfigurasi IDS yang digunakan adalah *Network-based Intrusion Detection System* (NIDS)
4. Sistem monitoring yang akan dibangun diaplikasikan pada sistem operasi Ubuntu dengan menggunakan Snort sebagai sistem pemonitor dan Telegram sebagai media pengiriman notifikasinya.
5. Pembuatan sistem ini tidak membahas uji coba jenis-jenis serangan yang dilakukan ke jaringan secara lebih mendalam.

6. Sistem hanya mengambil beberapa *sample* penyusupan dan tidak menjelaskan tindak lanjut dari administrator setelah mendapat notifikasi melalui Telegram.
7. Variabel Kemanan yang akan diteliti adalah tentang Keamanan sistem Komputer.
8. Metode Pengembangan sistem menggunakan metode PPDIOO *(Prepare, Plan, Design, Implement, Operate, Optimize)*.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud

Adapun maksud dari penelitiaan ini antara lain :

1. Sebagai prasyarat untuk kelulusan Program Studi Strata 1 Universitas Amikom Yogyakarta.

1.4.2 Tujuan

Adapun tujuan dari penelitian ini antara lain :

1. Menganalisis masalah keamanan jaringan yang ada pada SMA Negeri 11 Yogyakarta.
2. Mengimplementasikan *Network-based Intrusion Detection System* pada SMA Negeri 11 Yogyakarta.
3. Memberikan informasi ketika terjadi serangan secara *realtime* kepada administrator melalui Aplikasi *instant messaging* Telegram.

1.5 Manfaat Penulisan

a. Bagi Objek

Mendapatkan informasi berupa notifikasi kepada administrator melalui Telegrm ketika terjadi serangan.

b. Bagi Ilmu Pengetahuan

1. Mengetahui bagaimana implementasi *Network-based Intrusion Detection System.*
2. Mengetahui implementasi sistem untuk notifikasi apabila ada penyerangan ke Telegram.

1.6 Metode Penelitian

Langkah-langkah dalam melakukan penelitian yang berjudul "Analisis dan Implementasi Keamanan Jaringan menggunakan Network based Intrusion Detection System studi kasus SMA Negeri 11 Yogyakarta" ini dilakukan dengan metodologi berikut :

1.6.1. Studi Kepustakaan

Studi pustaka dilakukan untuk mempelajari dan mendapat pengetahuan dari bukum jurnal internet atau *literature* yang berhubungan dengan *Intrusion Detection System* dan pendeteksian serangan *cyber* dengan *Intrusion Detection System* sebagai dasar teori dalam perancangan sistem.

1.6.2. Metode Studi Sejenis

Melakukan pengumpulan data dengan mempelajari penelitian-penelitian sebelumnya yang memiliki karakteristik sama, baik dari segi teknologi maupun objek penelitian.

1.6.3. Metode Pengembangan Sistem

Metode pengembangan sistem menggunakan metode PPDIOO *life cycle* yang terdiri dari *Prepare, Plan, Design, Implement, Operate, Optimize.*

Adapun Rincian dari masing-masing proses tersebut antara lain :

1. *Prepare*

   Tahap yang pertama adalah prepare atau persiapan. Dimulai dari analisis alur dari penelitian yang akan dilakukan kemudian melakukan persiapan mengenai gambaran umum dari sistem yang akan dibangun.

2. *Plan*

   Pada tahap ini mengidentifikasi kebutuhan dari sistem yang akan dibangun seperti kebutuhan perangkat keras dan kebutuhan perangkat lunak.

3. *Design*

   Dalam tahapan ini membahas tentang detil logis perancangan arsitektur topologi yang sesuai dengan mekanisme sistem. Pada tahap ini akan dibuat perancangan menggunakan *flowchart* unuk menggambarkan mekanisme kerja serta topologi jaringan sistem detekdi serangan *cyber* dengan *Network-based Intrusion Detection System* pada SMA Negeri 11 Yogyakarta yang akan dibuat berdasarkan analisis.

4. *Implementation*

   Tahap selanjutnya adalah tahap implementasi, pada tahap ini menerapkan semua yang telah dirancangkan. Dalam tahap ini mencakup instalasi serta

konfigurasi terhadap rancangan topologi, dan konfigurasi yang dilakukan pada masing-masing perangkat yang telah ditentukan.

5. *Operate*

   Pada tahap ini dilakukan pengujian terhadap sistem yang telah dibangun serta pembahasan terhadap hasil pengujian yang telah dilakukan.

1.6.4. Penarikan Kesimpulan

Pada tahap ini dilakukan penarikan kesimpulan berdasarkan analisis pada data hasil pengujian.

1.6.5. Pembuatan Laporan

Pada tahap ini dilakukan penyusunan laporan yang memuat seluruh proses pengerjaan Tugas Akhir yang disesuaikan dengan ketentuan yang telah ditetapkan.

1.6.6. Sistematika Penulisan

Dalam penyusunan laporan penelitian ini akan disajikan dalam bentuk bab, antara lain sebagai berikut :

BAB I. PENDAHULUAN

Bab ini akan mebahas latar balakang, perumusan masalah, maksud dan tujuan penelitian, batasan batasa masalah dalam penelitian, metode penyelesaian masalah serta sistematika penulisan.

BAB II. LANDASAN TEORI

Pada bab ini akan membahas dan menjelaskan mengenai dasar teoritis yang menjadi landasan dan mendukung pelaksanaan penulisan laporan penelitian.

BAB III. ANALISIS DAN PERANCANGAN

Pada bab ini dibahas mengenai analisis rancagan sistem yang akan dibangun serta scenario pengujian yang akan dilakukan pada sistem.

BAB IV. HASIL DAN PEMBAHASAN

Bab ini membahas tentang proses implementasi mulai dari instalasi dan konfigurasi serta pengujian terhadap sistem yang telah dibangun. Pengujian berdasarkan skenario-skenario yang dibahas pada bab 3.

BAB V. PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilaksanakan dan saran saran dari masalah yang terkait untuk mengembangkan sistem yang lebih baik lagi terhadap penelitian selanjutnya.