BAB I

PENDAHULUAN

1.1 Latar Belakang

PT. GIT Solution (GITS) adalah salah satu perusahaan yang bergerak di bidang teknologi lebih tepatnya pada jasa perencanaan pembangunan dan pengembangan sistem informasi yang berskala nasional dan siap bersaing di kancah internasional. Gits sudah banyak menciptakan *software-software* yang dibutuhkan para *client*nya. Karena perusahaan ini juga memiliki beberapa divisi diantaranya ada *software development*, *game development*, *training center* dan juga divisi baru yaitu *digital marketing* yang bergerak dibidang jasa.

Namun, dari sekian banyak perkembangan yang ada di perusahaan ini tidak diiringi dengan keamanan jaringan yang mumpuni. Padahal jaringan perusahaan ini terhubung ke *server* yang notabennya bisa membahayakan data-data *client* maupun informasi-informasi yang bersifat *private* di perusahaan ini. Hal-hal yang seperti ini yang dapat mengakibatkan masalah yang patut dipertimbangkan, sebagaimana kita tahu serangan-serangan seperti *DDoS Attack, Port Scanning, Spoofing, Sniffing, FTP brute force, Malware* atau pun serangan-serangan yang lain dapat mengancam keamanan jaringan di perusahaan tersebut.

Oleh karena itu, perlu adanya dibangun suatu sistem keamanan jaringan yang dimana dapat memantau lalu lintas jaringan serta mengamati aktivitas jaringan yang berjalan secara *realtime,* yang mana jika terjadi serangan akan langsung diteruskan kepada administrator jaringan sebagai *alert* untuk ditindak lanjuti kemudian. *Network-Based Intrusion Detection System (NIDS)*

merupakan salah satu cara yang dapat diambil untuk menyelesaikan permasalahan yang ada.

Network-Based Intrusion Detection System (NIDS) merupakan suatu sistem yang dirancang untuk dapat memantau dan mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan tertentu. NIDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan kemudian mencari bukti dari percobaan intrusi (penyusupan). Jadi, seluruh paket yang masuk kedalam jaringan tersebut akan dibandingkan oleh *detection engine* apakah sesuai dengan *rules* yang sudah dimasukkan atau tidak. Apabila sesuai *rules* maka akan memberikan informasi kepada administrator berupa *alert* melalui BASE dan *telegram messages* bahwa telah terjadi serangan didalam jaringannya. Jika tidak sesuai dengan *rules* maka paket akan diteruskan masuk ke dalam jaringan.

Berdasarkan pemaparan dan penjelasan masalah di atas maka penulis melakukan penelitian yang berjudul "Analisis dan Implementasi Sistem *Network-Based Intrusion Detection System* (NIDS) Menggunakan *Snort* dengan Notifikasi Telegram Untuk Keamanan Jaringan di PT. GIT Solution".

1.2 Rumusan Masalah

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

1. Bagaimana membuat sistem yang dapat berfungsi untuk memonitoring keamanan jaringan?

2. Bagaimana notifikasi yang akan dikirimkan ke administrator ketika terjadi gangguan atau pun serangan pada jaringan tersebut?
3. Apa pengaruh implementasi NIDS ini jika dilihat dari sisi keamanan jaringan di PT. GITSolution?

1.3 Batasan Masalah

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

1. Sistem ini hanya ditujukan pada PT. GIT Solution
2. Jenis konfigurasi IDS yang digunakan adalah *Network-Based Intrusion Detection System (NIDS)*.
3. Sistem operasi yang digunakan adalah Ubuntu 16.04
4. IDS yang digunakan adalah *Snort v2.9.9.0*
5. Sistem yang akan dibuat diaplikasikan pada sistem operasi Ubuntu dengan menggunakan *Snort* untuk memonitoring keamanannya dan *Bot Telegram* hanya mengirimkan notifikasi serangan kepada administrator.
6. Serangan yang digunakan dalam pengujian ini adalah *Port Scanning, FTP Brute Force, SSH Login Attempt, DDoS Attack.*
7. 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 penelitian ini dibuat antara lain :

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

1.4.2 Tujuan

Adapun tujuan dari penelitian ini diantaranya adalah :

1. Menganalisis masalah keamanan jaringan yang ada di PT GIT Solution.
2. Mengimplementasikan *Network-based Intrusion Detection System* di PT. GIT Solution.
3. Memberikan alert atau pemberitahuan kepada administrator jika terjadi serangan secara *realtime* melalui *messaging Telegram*.

1.5 Manfaat Penulisan

1. Bagi Penulis
   a. Membuat karya tulis yang lebih bermanfaat.
   b. Memberikan pengalaman dan ilmu dalam membangun sistem keamanan jaringan melalui sistem operasi *Linux*.
2. Bagi Pembaca
   a. Sebagai acuan dalam penyusunan penelitian yang serupa.
   b. Sebagai referensi dalam membangun sistem keamanan jaringan terutama di *Linux*.

3. Bagi Objek
   a. Mendapatkan informasi notifikasi jika terjadi serangan kepada administrator.

1.6 Metode Penelitian

Metode penelitian yang akan digunakan dalam penelitian ini adalah sebagai berikut :

1.6.1 Studi Kepustakaan

Studi pustaka dilakukan untuk mempelajari dan mendapat pengetahuan dari buku jurnal internet atau *literature* yang berhubungan dengan *Intrusion Detection System* dan pendeteksian serangan keamanan jaringan 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* untuk menggambarkan mekanisme kerja serta topologi jaringan sistem deteksi serangan *cyber* dengan *Network-based Intrusion Detection System* di PT GITSolution 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.

1.7 Sistematika Penulisan

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

1.7.1 BAB I PENDAHULUAN

Bab ini berisi penjelasan mengenai latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika pada penulisan ini.

1.7.2 BAB II LANDASAN TEORI

Bab ini berisi penjelasan mengenai landasan teori yang digunakan diantaranya tinjauan pustaka, konsep dan teori serta perangkat lunak yang akan digunakan dalam perancangan dan pembangunan *sistem monitoring* menggunakan *snort* pada penelitian ini.

1.7.3 BAB III ANALISIS DAN PERANCANGAN

Pada bab ini dibahas mengenai analisis rancangan sistem yang akan dibangun serta skenario pengujian yang akan dilakukan pada sistem.

1.7.4 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.

1.7.5 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.