

BAB I

PENDAHULUAN

1.1 Latar Belakang

PT Telekomunikasi Indonesia Tbk biasa disebut Telkom Indonesia merupakan perusahaan Badan Usaha Milik Negara (BUMN) yang bergerak dalam bidang informasi dan komunikasi serta penyedia jasa jaringan telekomunikasi dan jaringan internet.

Seiring perkembangan teknologi yang sangat pesat menuntut meningkatnya kualitas keamanan jaringan, terutama dengan semakin terbukanya pengetahuan tentang *hacking* dan *cracking*, dalam meningkatkan pelayanan keamanan jaringan sangat penting untuk menjaga *validitas* dan *integritas* data. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak bertanggung jawab.

Penanganan gangguan saat ini umumnya dilakukan secara manual oleh para *administrator*. Hal ini mengakibatkan sistem bergantung pada ketersediaan dan kecepatan *administrator* dalam merespons gangguan. Apabila gangguan tersebut berhasil membuat suatu jaringan mengalami masalah, maka sistem tidak dapat di pulihkan dengan cepat.

Banyak masalah yang sering terjadi pada keamanan jaringan di karenakan sering terjadi *Backdoor*, *Port Scan*, *Virus dan Malware*, *Hacker/Craker*, *Denial of Servis (Dos/DDos, ping of Dead* yang dapat mengakibatkan lemahnya sistem

keamanan jaringan. Untuk mengatasi masalah keamanan jaringan computer perlu adanya penerapan pengawasan dalam sebuah jaringan komputer, maka perlu di terapkan *system monitoring* yaitu *Intrusion Detection System (IDS)*.

Intrusion Detection System (IDS) adalah metode pendeteksi aktivitas yang mencurigakan dalam sebuah system jaringan dengan menggunakan suatu perangkat lunak (*software*) yang bekerja secara otomatis untuk memonitor keadaan jaringan komputer dan dapat menganalisis masalah keamanan jaringan.

Salah satu alternatif kebutuhan spesifikasi (*hardware*) yang tinggi adalah dengan memanfaatkan *Raspberry Pi*. *Raspberry Pi* merupakan komputer mini yang memiliki ukuran kecil tetapi mampu menjalankan tugas yang sama dengan komputer.

Menurut (Alamsyah, 2011) *Snort* adalah *Intrusion Detection System* jaringan *open source* yang mampu menjalankan analisis *real-time* dan paket *logging* pada *IP network*. *Snort* dapat menjalankan analisis protokol, *content searching* atau *maching*, dan dapat digunakan untuk mendeteksi berbagai serangan dan penyusupan.

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusupan maupun menganalisa paket yang melintasi jaringan secara *realtime traffic*, serta mampu mendeteksi berbagai serangan yang berasal dari jaringan luar. *Snort* dapat digunakan pada *platform* sistem operasi Linux, BSD, Solaris, Windows dan sistem operasi lainnya.

Berdasarkan latar belakang di atas maka penulis tertarik untuk meneliti dan menyusun sebuah penelitian yang berjudul **“PENERAPAN *INTRUSION DETECTION SYSTEM* SEBAGAI SISTEM KEAMANAN JARINGAN INTERNET BERBASIS *RASPBERRY PI*”**.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dikemukakan maka dapat diidentifikasi beberapa permasalahan sebagai berikut.

1. Masih lemahnya sistem keamanan jaringan yang mengakibatkan sering terjadinya koneksi lambat dan sering mengalami *request time out* terus menerus.
2. Sistem pertahanan terhadap gangguan saat ini dilakukan secara manual oleh para *administrator*.
3. Masalah yang sering terjadi pada keamanan jaringan di karenakan *Virus dan Denial of Servis (Dos/Ddos)*, yang dapat mengakibatkan lambatnya koneksi suatu jaringan.

1.3 Batasan Masalah

Berdasarkan identifikasi masalah di atas ruang lingkup batasan masalah dalam laporan penelitian ini hanya terbatas pada masalah-masalah sebagai berikut:

1. *Raspberry pi* menggunakan sistem operasi *Linux*.
2. *Tools* yang digunakan untuk memonitoring menggunakan *Software Snort*.
3. Peneliti hanya membahas tentang keamanan jaringan internet.

1.4 Perumusan Masalah

Dengan memperhatikan identifikasi masalah diatas, maka permasalahan yang akan dipecahkan dalam penulisan penelitian ini adalah ;

1. Bagaimana membangun suatu system *Intrusion Detection System* (IDS) sebagai keamanan jaringan internet berbasis *Raspberry pi*.
2. Bagaimana membangun suatu sistem kemanan jaringan internet yang secara otomatis mendeteksi suatu gangguan berbasis *Raspberry pi*.
3. Bagaimana cara *Intrusion Detection System* (IDS) mendeteksi setiap serangan yang terjadi didalam *system* jaringan.

1.5 Tujuan Penelitian

Sesuai dengan perumusan masalah yang dikemukakan di atas, tujuan penelitian ini sebagai berikut.

1. Mengimplementasikan *Intrusion Detection System* (IDS) sebagai *system* keamanan jaringan internet berbasis *Raspberry pi*.
2. Untuk mempermudah *administrator* dalam mengamankan jaringan internet dari gangguan secara otomatis.
3. Mendeteksi semua serangan yang masuk dari jaringan internet menggunakan *software snort* yang berbasis *Raspbery pi*.

1.6 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat secara teoritis bagi kemajuan dan perkembangan keamanan jaringan internet.

1.6.1 Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan manfaat secara teoritis bagi kemajuan dan perkembangan ilmu pengetahuan dalam keamanan jaringan, Khususnya untuk Telkom Batam.

1.6.2 Manfaat Praktis

Manfaat yang di dapatkan dari penelitian ini sebagai berikut :

1. Bagi penulis

Menambah wawasan mengenai *Intrusion Detection System* (IDS) sebagai *system* keamanan jaringan internet berbasis *Raspberry pi*.

2. Bagi perusahaan

Mempermudah *administrator* dalam memonitor jaringan komputer dari ancaman dan usaha penyusupan dari pihak yang tidak memiliki hak akses atau tidak berwenang.

3. Bagi ilmu pengetahuan

Adanya penelitian ini, maka dapat dijadikan dasar pengembangan tentang *Intrusion Detection System* (IDS) sebagai sistem keamanan jaringan berbasis *Raspberry pi* bagi peneliti berikutnya.