BAB I

PENDAHULUAN

1.1 Latar Belakang

Era modern membuat masyarakat berbondong-bondong untuk menggunakan berbagai teknologi yang sudah canggih, sebisa mungkin mereka menggunakannya kapanpun dan dimanapun. Oleh karena itu, pengguna teknologi membutuhkan jaringan internet yang memumpuni. Sekarang jaringan internet sudah tersedia di banyak tempat terutama tempat umum agar dapat digunakan oleh mereka yang tidak sengaja singgah atau memang ingin mencari jaringan internet umum.

Jaringan internet yang terhubung dengan banyak orang pada dasarnya tidak aman dan memungkinkan dieksploitasi *hacker*. Maka, keamanan jaringan internet menggunakan *Wireless* menjadi sangat penting dan perlu untuk diperhatikan.

Pada saat terjadi komunikasi antar data, data akan melewati beberapa teminal untuk sampai kepada penerima. Itu berarti akan memberikan kesempatan kepada pengguna yang tidak bertanggung jawab untuk melakukan penyadapan atau mengubah data tersebut. Perancangan sistem keamanan jaringan wireless harus direncanakan dan dipahami dengan baik dan benar agar dapat melindungi sumberdaya yang berada dalam jaringan tersebut serta meminimalisir serangan yang tidak diinginkan.

Terbukanya pengetahuan tentang *hacking* dan *cracking* yang mudah didapatkan pada tools yang bisa digunakan dengan mudah dan gratis. Selain itu ancaman keamanan jaringan bisa terdapat oada virus, *malicious, trojan, worm, spamming* dan lainnya. Hal ini dapat mengancam keamanan sistem jaringan.

Sistem keamanan jaringan *wireless* yang terhubung ke internet dengan baik dapat melindungi sumberdaya yang berada di dalam jaringan tersebut secara efektif. Serangan yang dilakukan oleh hacket ada beberapa jenis antara lain, *packet sniffer, ARP spoofing, probe, scan account compromise, Root compromise* dan *Denial of Service(DOS).* Salah satu ancaman yang bisa menyerang pengguna fasilitas access point adalah serangan *packet sniffing.*

Packet sniffing adalah teknik pemantauan setiap paket yang melewati jaringan dan bagian dari perangkat lunak atau perangkat keras yang memonitor semua lalulintas pada jaringan. *Packet sniffing* berpotensi hilangnya privasi dan infornasi penting bisa tercuri ataupun rahasia yang dimiliki pengguna.

Banyak metode yang dapat dilakukan untuk mengamankan sebuah sistem jaringan. Salah satunya adalah *Intrusion Detection System(IDS).* IDS merupakan perangkat yang memonitor jaringan atau sistem untuk melihat kegiatan yang mencurigakan atau pelanggaran kebijakan dan memberikan laporan ke administrator.

Saat melakukan serangan *packet sniffing* banyak *tools* yang dapat digunakan. Dalam penelitian ini dilakukan proses *sniffing* menggunakan

software bettercap pada OS KaliLinux. Dengan penggunaan *bettercap* dapat digunakan untuk melihat aktivitas jaringan yang sedang digunakan.

Untuk mengatasi permasalahan perlu sebuah mekanisme keamanan jaringan untuk medeteksi serangan *packet sniffing* pada jaringan menggunakan *Intrusion Detection Sytem(IDS)* sehingga dapat memonitoring dan melakukan drop ketika terjadi aktivitas jaringan yang mencurigakan.

Hasil dari monitoring menggunakan Snort akan diteruskan ke Splunk agar memudahkan untuk dipahami. Kemudian log dari Splunk akan dipergunakan untuk mengirimkan notifikasi email agar dapat ditelaah oleh administrator

1.2 Rumusan Masalah

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

1. Bagaimanakah cara mengidentifikasi serangan *packet sniffing*?
2. Bagaimanakah cara metode Snort bekerja agar dapat mengirimkan notifikasi?
3. Bagaimanakah cara user mengetahui kalau jaringannya terkena serangan *packet sniffing*?

1.3 Batasan Masalah

Untuk mempermudah dan menyederhanakan pemahaman yang dibahas maka perlu adanya batasan masalah, sebagai berikut :

1. Penelitian ini hanya membahas tentang metode IDS terhadap serangan *packet sniffing* terkait monitoring jaringan.

2. Penelitian ini hanya menjelaskan bagaimana cara melihat log notifikasi serangan *packet sniffing* yang dikirimkan oleh splunk.
3. Implementasi keamanan jaringan meliputi monitoring menggunakan bettercap di KaliLinux, melakukan penerapannya menggunakan Snort dan melihat laporannya di Email.

1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan dari penyusunan penelitian ini diantaranya :

1. Sebagai salah satu syarat menyelesaikan pendidikan program studi strata 1 jurusan Informatika di Universitas AMIKOM Yogyakarta dengan gelar sarjana komputer (S.Kom).
2. Mampu merancang dan mengimplementasi keamanan jaringan yang bisa berguna untuk oranglain.
3. Menerapkan konfigurasi untuk mengimplementasi monitoring jaringan dan menjaga jaringan agar aman dari orang yang tidak bertanggung jawab.
4. Menambah wawasan tentang teknologi keamanan jaringan.

1.5 Manfaat Penelitian

1. Bagi Penulis
   a. Memperoleh gelar Sarjana Komputer di Universitas AMIKOM Yogyakarta.
   b. Menambah wawasan bagi penulis mengenai keamanan jaringan dengan metode *Intrusion Detection System(IDS)*.
   c. Pembuatan karya ilmiah turut sebagai bukti yang berperan serta dalam pengembangan ilmu pengetahuan khususnya bidang IT.
2. Bagi Pembaca
   a. Dapat menambah informasi mengenai keamanan jaringan dengan metode IDS.
   b. Sebagai pertimbangan saat menentukan keamanan jaringan untuk *packet sniffing*.

1.6 Metode Penelitian

Dalam menyusun penelitian skripsi ini ada beberapa metode yang digunakan, antara lain :

1. Metode Pustaka

   Merupakan metode yang dilakukan untuk mencari dan mempelajari segala kajian pustaka yang memiliki keterkaitan dengan tema penelitian. Pengambilan data bersumber dari buku, internet dan penelitian sebelumnya yang mendukung teori yang berkaitan.

2. Metode Observasi

   Dengan melakukan percobaan atau pengetesan metode yang akan dijalankan

1.6.1 Metode Perancangan dan Analisa Sistem

Pada penelitian ini, penulis melakukan sistem kerja sebagai berikut :

Gambar 1.6.1 Sistem Kerja

Maksud dan penjelasan sistem kerja dalam penelitian ini adalah sebagai berikut :

1. Perancangan

   Tahap ini merupakan tahap awal yang dilakukan untuk meneliti, meninjau, mempersiapkan dan mengidentifikasi sistem.

2. Konfigurasi dan Implementasi

   Menginstall aplikasi yang akan digunakan, setelah itu melakukan instalasi lalu melakukan konfigurasi terhadap aplikasi Snort yang berguna untuk mengamati aktivitas dalam suatu jaringan, aplikasi *Bettercap* yang akan digunakan untuk menganalisis kinerja jaringan, lalu-lintas jaringan komputer, transmisi paket data dalam jaringan dan membaca data secara langsung dan Email akan digunakan untuk melihat notifikasi hasil monitoring jaringan.

3. Uji Coba

   Melakukan pengujian dengan menggunakan PC penyerang dan PC pendeteksi yang sudah terhubung ke *access point*. PC penyerang akan melakukan serangan *packet sniffing* terhadap *access point*. Kemudian log hasil penyerangan akan dikirimkan ke Splunk lalu akan diteruskan sebagai notifikasi ke Email.

4. Hasil

Penulis melakukan analisa terharap hasil uji coba serangan *packet sniffing* dan mendeteksi serangan menggunakan IDS.

1.7 Sistematika Penulisan

Sistematika penulisan yang dilakukan dalam menyelesaikan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini membahas latar belakang, rumusan masalah, batasan masalah, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini akan membahas dan menjelaskan tentang landasan teori mengenai keamanan jaringan dari serangan *packet sniffing* dan metode *Intrusion Detection System(IDS)*.

BAB III ANALISIS DAN PERANCANGAN

Dalam bab ini akan membahas dan menjelaskan tentang hasil analisa permasalahan yang diperoleh dari proses perancangan keamanan jaringan *packet sniffing* dengan *Intrusion Detection System(IDS)* yang akan di implementasikan.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Dalam bab ini akan membahas dan menjelaskan tentang rancangan keamanan jaringan dari serangan *packet sniffing* dan implementasi *Intrusion Detection System(IDS)* dari hasil pengamatan, evaluasi dan pengujian sistem yang sudah jadi.

BAB V PENUTUP

Pada bab ini berisikan tentang kesimpulan dan saran.