BAB I

Pendahuluan

1.1. Latar Belakang Masalah

Jaringan komputer adalah sekelompok dua atau lebih komputer yang terhubung dan saling berhubungan, sehingga dapat bertukar informasi serta dapat berkomunikasi antara satu perangkat dengan perangkat jaringan lainnya. Adanya jaringan komputer memberikan manfaat pada aktivitas manusia, contohnya seperti antar manusia dapat berkomunikasi menggunakan *video call*, *instan messenger, email* dan dapat melakukan *sharing printer*. Menurut Zymon Machajewski bahwa Jaringan komputer adalah sekelompok perangkat atau peranti yang saling terhubung dan berinteraksi dengan komputer lainnya, untuk tujuan berbagi sumber daya [1].

Sebuah jaringan komputer harus dapat memberikan rasa aman terhadap pengaksesan yang dilakukan oleh seorang pengguna, ini berkaitan dengan tiga pilar keamanan jaringan yaitu CIA yang merupakan singkatan *Confidentiality* yaitu Kerahasiaan, *Integrity* yaitu Integritas, dan *Availability* yaitu Ketersediaan, dengan menerapkan dasar pilar tersebut sudah menjadi acuan untuk memberikan jaminan keamanan informasi atau data pribadi dari pengaksesan ilegal oleh pengguna yang tidak berkepentingan seperti *intruder* (Penyerang).

Keamanan jaringan merupakan salah satu faktor pada sebuah sistem untuk menjamin terjaganya kevalidan dan integritas data serta tersedianya layanan untuk pengguna. Sistem keamanan jaringan harus terlindungi dari berbagai macam akses jaringan yang tidak sah khususnya dari jaringan luar (Internet) [2].

Tujuan utama keamanan jaringan yaitu mengantisipasi ancaman yang dapat berupa ancaman fisik maupun ancaman non-fisik yang dapat mengganggu lalu lintas jaringan, kinerja dan konfigurasi pada perangkat yang ada dalam jaringan.

Salah satu metode untuk menjaga keamanan jaringan adalah dengan menggunakan sistem deteksi intrusi (*Intrusion Detection System*/IDS) yang telah dikembangkan oleh Martin Roesch. [3]. IDS dapat digunakan untuk memonitoring lalu lintas jaringan, terutama lalu lintas yang masuk dari jaringan luar ke jaringan lokal. Monitoring jaringan dapat menjadi tindakan pertama bagi seorang administrator untuk mengetahui jenis serangan apa saja yang dilancarkan oleh *intruder* apabila terjadi insiden penyerangan, sehingga administrator dapat segera mengambil tindakan pencegahan yang cepat dan tepat untuk mengatasi serangan tersebut. Namun memonitoring keamanan jaringan selama 24 jam akan sulit bagi seorang administrator dan serangan yang dilancarkan oleh *intruder* tidak memandang waktu, sehingga ada kemungkinan saat insiden serangan terjadi, administrator tidak sedang memonitoring keamanan jaringan, hal ini dapat menyebabkan kurang cepatnya pencegahan untuk mengatasi serangan tersebut yang dapat berakibat fatal pada perangkat jaringan. Seperti matinya perangkat server, menurunnya kinerja dari perangkat jaringan atau bahkan dapat memberikan waktu bagi *intruder* untuk menemukan celah keamanan jaringan yang fatal sehingga perangkat jaringan dapat diretas.

Studi literatur yang dilakukan pada beberapa jurnal dengan penelitian sistem deteksi serangan keamanan jaringan, menemukan bahwa masih kurangnya penelitian yang berfokus untuk mendeteksi satu jenis serangan keamanan jaringan dengan macam-macam variasi variabelnya dan ditemukan juga bahwa hasil konfigurasi sistem deteksi serangan keamanan jaringan yang dibuat menunjukan pesan peringatan *false positif* ketika terjadi insiden serangan keamanan jaringan, artinya sistem dapat mendeteksi

serangan namun salah dalam mengidentifikasi jenis serangan keamanan jaringan yang terjadi.

Berdasarkan permasalahan diatas maka judul yang dapat diangkat yaitu "Rancang Bangun Sistem Monitoring Keamanan Jaringan Universitas Ahmad Dahlan Melalui Aplikasi Mobile Berbasis Android Menggunakan Metode *Intrusion Detection System*". Penelitian ini berfokus pada pengembangan sistem yang dapat mendeteksi dengan akurat sesuai jenis serangan dan akan mengirimkan pesan peringatan kepada adminstrator jaringan secara *realtime* apabila terjadi insiden serangan, salah satu cara tersebut yaitu membuat sistem dengan memanfaatkan Snort *intrusion detection system* (IDS) yang dikolaborasikan dengan aplikasi mobile berbasis *android* untuk menampilkan informasi serangan dalam bentuk statistik. Sehingga ketika terjadi insiden serangan yang dilancarkan oleh *intruder* (penyerang) administrator akan mendapatkan sebuah notifikasi peringatan dari jaringan yang dikelola dan dapat melihat statistik serangan yang terjadi pada aplikasi. Dengan berbekal notifikasi informasi serangan tersebut administrator dapat menentukan tindakan pencegahan yang tepat dan cepat.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah diatas, maka dapat dirumuskan rumusan masalah sebagai berikut:

1. Bagaimana cara mendeteksi serangan keamanan jaringan yang umum dilancarkan oleh penyerang?
2. Bagaimana membuat sistem yang dapat mengirimkan notifikasi peringatan ke perangkat *mobile* administrator saat terjadi insiden serangan keamanan jaringan?

3. Apakah konfigurasi yang dilakukan dengan memanfaatkan IDS mampu mendapatkan persentase dengan akurasi yang tinggi dalam mendeteksi serangan keamanan jaringan?

1.3. Tujuan Penelitian

Berikut adalah tujuan yang ingin dicapai dalam penelitian ini:

1. Mengetahui serangan keamanan jaringan yang dilancarkan pada jaringan UAD.
2. Membuat sistem yang dapat memonitoring keamanan jaringan UAD melalui Snort IDS lalu akan ditampilkan statistiknya pada aplikasi *mobile* berbasis android.
3. Membuat sistem yang dapat menampilkan notifkasi peringatan melalui aplikasi dan SMS.
4. Mendapatkan persentase dengan akurasi yang tinggi untuk mendeteksi pola serangan keamanan jaringan UAD menggunakan Snort *IDS*.

1.4. Batasan Masalah Penelitian

Penelitian ini membahas rancang bangun sistem monitoring keamanan jaringan dengan batasan masalah sebagai berikut:

1. Luas lingkup simulasi dalam penelitian hanya meliputi jaringan lokal Universitas Ahmad Dahlan
2. Penelitian menggunakan IDS (*Intrusion detection system)* sebagai metode deteksi lalu lintas pada jaringan lokal.
3. Snort akan bekerja sebagai IDS *(Instrusion detection system)* untuk memonitoring seluruh aktivitas jaringan yang sedang berlangsung.
4. Luas lingkup simulasi serangan yang akan dilakukan hanya meliputi serangan *Denial of Service* (DoS) dan *Port Scanning* dengan target website Universitas Ahmad Dahlan.

5. Sistem yang dibuat ditujukan pada sistem operasi *Android* dengan format apk.
6. Sistem Aplikasi pada Android digunakan untuk menampilkan informasi statistik serangan yang terdeteksi.

1.5. Manfaat Penelitian

Diharapkan bahwa penelitian ini akan memberikan keuntungan atau manfaat bagi pihak-pihak sebagai berikut:

1. Bagi UAD
    - Sistem yang dibuat, diharapkan dapat memberikan kontribusi untuk meningkatkan kesadaran akan pentingnya keamanan jaringan.
    - Membantu administrator jaringan untuk melakukan monitoring keamanan jaringan.
2. Bagi Akademisi
    - Menambah informasi tentang keamanan jaringan khususnya bagi administrator jaringan.
    - Memberikan gambaran sebuah sistem monitoring keamanan jaringan.
    - Menambah ilmu tentang bagaimana sistem dapat mendeteksi serangan pada jaringan komputer.