Chapter 1

Pendahuluan

1.1 Latar Belakang

Sistem keamanan Jaringan merupakan hal yang sangat penting untuk dikembangkan untuk menjaga kerahasiaan dan keamanan data. Karena data merupakan hal yang sangat vital dalam kehidupan di zaman modern ini.

Akan tetapi seiring dengan perkembangan teknologi, semakin banyaknya *software* yang dikembangkan, sehingga banyak pula celah keamanan yang timbul. Sehingga, kebutuhan dalam teknologi keamanan jaringan menjadi sangat banyak pula.

1.1.1 Data terkait

Dilansir dari *Kaspersky Securelist* persebaran virus terbesar dari periode pelaporan Trojan-Banker.AndroidOS.Asacub. Ini memuncak pada bulan September ketika lebih dari 250.000 pengguna diserang - dan semua itu hanya mencakup statistik bagi mereka yang memiliki produk seluler Kaspersky Lab yang diinstal pada perangkat mereka.

[width=]skripsi/1statistik figureJumlah pengguna yang diserang oleh mobile banker Asacub pada tahun 2017 dan 2018 [**?**]

Dari data diatas dapat diamati bahwa penyebaran virus jenis Trojan-Banker ini selalu meningkat.

1.1.2 Penelitian terkait

1.2 Rumusan Masalah

Dari latar belakang dapat dirumuskan masalah sebagai berikut:

1. Bagaimana karakteristik intrusi *Binary Virus* yang dapat dideteksi dan tidak dapat dideteksi oleh IDS ?

2. Bagaimana proses pemodelan *Recurrent Neural Network* untuk mendeteksi intrusi *Binary Virus* pada jaringan ?

3. Bagaimana proses optimasi *Recurrent Neural Network* untuk memprediksi intrusi *Binary Virus* pada jaringan ?

4. Bagaimana hasil prediksi pemodelan *Recurrent Neural Network* untuk memprediksi intrusi *Binary Virus* pada jaringan ?

1.3 Batasan Masalah

1. Jenis malware yang di analisis merupakan malware berjenis *Binary Virus* dengan metode pendeteksian *signature*

2. RNN digunakan untuk memprediksi kecenderungan intrusi

3. IDS diuji tanpa mengaktifkan rule dari *preprocessor* lain

4. IDS di implementasikan pada jaringan lokal (LAN)

1.4 Tujuan

1. Mengintegrasikan kecerdasan buatan dalam penerapannya di bidang keamanan jaringan

2. Meningkatkan kapabilitas sistem keamanan jaringan untuk pendeteksian intrusi dengan metode RNN

3. Mengukur kemampuan RNN dalam melakukan pendeteksian dan penyaringan data pada IDS

4. Mengoptimalkan efektifitas kinerja RNN dalam pendeteksian virus dan otomasi rule pada IDS

1.5 Manfaat

1. Memberikan kemudahan dalam pendeteksian intrusi *Binary Virus*

2. Menjadi referensi untuk mengimplementasikan sistem RNN pada IDS

3. Menjadi solusi untuk kegiatan pencarian pola untuk dijadikan rule atau tidak

1.6 Sistematika Penulisan

Untuk mencapai tujuan yang diharapkan, maka sistematika penulisan yang disusun dalam tugas akhir ini dibagi menjadi 5 bab sebagai berikut :

- Bab I. Pendahuluan
  Bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan
- Bab II. Tinjauan Pustaka dan Landasan Teori
  Bab ini memuat tentang tinjauan pustaka yang menjabarkan hasil penelitian yang berkaitan dengan penelitian ini dan landasan teori yang menjabarkan teori-teori penunjang yang berhubungan dengan penelitian ini.
- Bab III. Metedologi Penelitian
  Memuat tentang metode penelitian, mulai dari pelaksanaan penelitian, diagram alir penelitian, menentukan alat dan bahan, lokasi penelitian, dan langkah-langkah penelitian.
- Bab IV. Hasil Penelitian
- Bab V. Penutup