

1. Pendahuluan

Pada bagian ini berisi empat sub-bagian yaitu: Latar Belakang, Topik dan Batasannya, Tujuan dan Organisasi Tulisan. Di bawah ini akan dijelaskan dari masing-masing sub-bagian tersebut.

Latar Belakang

Sistem Komunikasi merupakan hal yang tak terhindarkan di kehidupan sehari-hari. Jaringan Komputer efektif digunakan untuk pengolahan data bisnis, pendidikan, hiburan dan lain sebagainya. Seiring dengan perkembangan konsep jaringan membuatnya rentan terhadap serangan yang dilancarkan oleh para penyusup diantaranya adalah serangan DoS (Denial of Service) [1]. DoS (Denial of Service) adalah salah satu jenis serangan yang digunakan penyerang untuk membuat layanan tidak dapat diakses oleh pengguna yang sah. Dalam hal ini, terdapat beberapa jenis serangan diantaranya *TCP SYN attack*, *UDP flood attack* dan *ICMP flood attack*[2].

Pada [[3],[4], [5],[6],[7]] telah dilakukan penelitian untuk mendeteksi serangan DoS menggunakan dataset NSL-KDD untuk mendeteksi serangan. Berdasarkan pernyataan tersebut, maka dapat disimpulkan bahwa untuk mendeteksi DoS masih menggunakan dataset. Pada tugas akhir ini, berdasarkan dataset NSL-KDD akan dilakukan validasi traffic DoS, Trafik DoS yang digunakan adalah TCP, UDP, ICMP. Teknik validasi yang digunakan untuk melakukan validasi adalah Teknik validasi matematis dengan menggunakan pengujian validitas *pearson*.

Topik dan Batasannya

Pada penelitian ini penulis mengangkat permasalahan terkait bagaimana cara memvalidasi trafik serangan DoS di *live network*. Untuk penelitian ini penulis menggunakan dataset NSL-KDD sebagai acuan validasi. Dataset NSL-KDD merupakan pembaruan dari dataset KDDCUP-99 dan akhir-akhir ini banyak digunakan riset untuk menentukan akurasi deteksi serangan pada sebuah jaringan. Terdapat 41 Fitur yang terdapat NSL-KDD namun pada penelitian ini penulis hanya menggunakan 13 fitur yang telah diseleksi menggunakan *Information Gain*. Penulis hanya berfokus pada serangan yang berada pada layer 3 dan 4 atau layer *network* dan *transport*, dan trafik yang diamati diantaranya TCP,UDP dan ICMP.

Tujuan

Penelitian ini dilakukan dengan tujuan untuk menjadi rujukan peneliti selanjutnya dalam melakukan riset terhadap deteksi serangan DoS di *live network*.

Organisasi Tulisan

Selanjutnya, jurnal tugas akhir ini akan menjelaskan berbagai penelitian yang sudah pernah dilakukan sebelumnya serta hal-hal yang terkait dengan penelitian ini pada bagian II. Metode penelitian yang digunakan dan sistem yang dibangun pada proses klasifikasi akan dijelaskan pada bagian III. Pada bagian IV akan dijelaskan hasil yang diperoleh serta evaluasi dari penelitian yang telah dilakukan. Terakhir yaitu penarikan kesimpulan dan pemberian saran untuk penelitian kedepannya yang akan dijelaskan pada bagian V.