Metode deteksi serangan distributed denial of service menggunakan flow traffic dan algoritma self organizing map

Ahmad Sanmorino, author

Abstrak

Pembahasan mengenai serangan distributed denial of service menjadi salah satu topik utama dalam wacana keamanan internet. Walaupun penggunaannya sudah lebih dari satu dekade dan mekanisme atau cara kerjanya sudah dipahami secara luas, namun hingga saat ini masih sangat sulit untuk mendeteksi secara dini suatu serangan distributed denial of service. Lambatnya pendeteksian serangan distributed denial of service karena sulitnya membedakan antara paket normal dan paket yang berasal dari agen distributed denial of service. Kesulitan lainnya adalah besarnya jumlah paket yang dikirim, hal ini mengakibatkan lamanya waktu yang dibutuhkan untuk menganalisa, dan dapat menyebabkan akurasi pendeteksian serangan distributed denial of service menurun.
Melalui penelitian ini peneliti mencoba memberikan solusi yaitu berupa metode untuk mendeteksi serangan distributed denial of service. Adapun metode yang diajukan disini yaitu dengan melakukan pendeteksian secara dini ketika terjadi serangan distributed denial of service terhadap server jaringan. Dalam melakukan pendeteksian dibutuhkan metode yang efektif untuk segera memberikan peringatan atau informasi bahwa telah terjadi serangan distributed denial of service.
Metode yang peneliti ajukan adalah metode deteksi menggunakan algoritma self organizing map dengan memanfaatkan lalu-lintas flow pada jaringan dan menggunakan fitur perhitungan dari metode yang sudah ada sebelumnya, yaitu metode IP FLow. Berdasarkan hasil pengujian, metode yang diajukan berhasil meningkatkan akurasi dan mempercepat waktu deteksi serangan distributed denial of service dibandingkan metode IP Flow.
.....
Discussion about distributed denial of service attack to be one of the main topics on the Internet security discourse. Although it appearance was more than a decade and it works has been widely understood, but it is still very difficult to detect at early stage of distributed denial of service attack. The delay of distributed denial of service attack detection due to difficulties in distinguishing between normal packets and packets originating from distributed denial of service agents. Another difficulty is the huge number of packets sent, it causes the length of time required to analyze, and could lead to decrease accuracy of detection.
Through this study, researcher tried to provide a solution in the form of methods for detecting distributed denial of service attacks. The method proposed here is to perform early detection of a distributed denial of service attacks on a network server. Doing detection certainly needed an effective method for giving immediate warning or information that distributed denial of service attacks have occurred.
The proposed method research is the detection method using self organizing map algorithm based on flow traffic on the network and by using statistical calculation taken from existing method, IP Flow method. Based on test results, the proposed method successfully improves the accuracy and speed time detection of distributed denial of service attacks than using the IP Flow method.