Abstrak

Keamanan jaringan komputer menjadi bagian terpenting untuk menjamin integritas dan validitas layanan bagi pengguna. Suatu serangan ke dalam web server komputer dapat terjadi kapan saja. Salah satunya serangan *Flooding* yang merupakan ancaman serius keamanan jaringan pada web server dapat mengakibatkan kerugian *bandwidth* dan akses web lambat, baik bagi pengguna maupun penyedia layanan web server. Langkah awal untuk meminimalisir terjadinya serangan flooding adalah kemampuan untuk mendeteksi serangan dengan menggunakan *Intrusion Detection System* (IDS). Snort merupakan salah satu *tool* yang dapat digunakan untuk mendeteksi serangan *flooding*.

Snort memiliki kemampuan untuk mendeteksi serangan *flooding* secara *real time* dengan menerapakan *rule* khusus untuk menghasilkan suatu file log yang mencatat aktivitas yang dianggap berbahya. *File log* yang merupakan barisan data untuk menyimpan informasi mengenai segala tindakan, kejadian dan aktifitas yang terjadi di dalam sebuah sistem jaringan. Selanjutnya digunakan untuk proses investigasi analisis forensic jaringan (*network forensic*) yang merupakan ilmu keamanan komputer berkaitan dengan tahap-tahap untuk menemukan sumber serangan. Investigasi yang digunakan berupa model proses forensik. Terdiri dari tahap pengkoleksian, pemeriksaan, analisis dan pelaporan untuk mendapatkan bukti-bukti serangan yang bersumber dari file log.

Hasil penelitian yang telah dilakukan pemasangan *Intrusion Detection System* (IDS) Snort mampu mendeteksi serangan *flooding*. Sejumlah 15 IP *address* yang melakukan tindakan illegal ke dalam *web server*. Hasil analisis penelitian *flooding* dapat menemukan barang bukti investigasi menggunakan *Intrusion Detection System* (IDS) Snort. Berdasarkan hasil pengujian tersebut dapat dinyatakan hasil sudah sesuai dengan tujuan yang diharapkan, sehingga dapat disimpulkan penelitian ini berhasil berjalan dengan baik dan lancar.

Kata Kunci

serangan *flooding*, *intrusion detection system* (IDS), snort, *network forensic*.

Abstract

Computer Network Security Become The most important part to ensure the integrity and validity of the review SERVICE For users. To attack a web server hearts Computers can be Happen Anytime. One of Those Flood Attacks Which is a serious threat ON Network Security web server bandwidth can be resulted Losses And web Access Slow, both users and providers of those web server program service. Initial steps for the review minimize flood attack is the ability to detect attacks BY review using Intrusion Detection System (IDS). Snort is a prayer One That tool can be used to detect review flood attacks.

Snort has the ability to detect flooding attacks in real time by applying a special rule to generate a log file that records the activities that are considered berbahya. The log file which is a sequence of data to store information about all actions, events and activities that occur in a network system. Further investigation process used for forensic analysis of network (network forensic) which is the science of computer security with regard to the steps to find the source of the attack. Investigations are used in the form of the forensic process model. Comprising the step of collecting, examination, analysis and reporting to obtain evidence of attacks originating from the log files.

Results of research conducted installation of Intrusion Detection System (IDS) Snort is able to detect flooding attacks. Some 15 IP addresses that perform illegal actions to the web server. Results of analysis of flooding can find evidence in the investigation using Intrusion Detection System (IDS) Snort. Based on these test results can be declared results are in accordance with the expected goals, so that we can conclude this study managed to run well and smoothly.

Keywords

flooding attacks, intrusion detection system (IDS), snort, forensic network.