



INTISARI

PERINGATAN DINI SERANGAN JARINGAN KOMPUTER BERBASIS *GENERATED RULES DAN LOG HONEYD*

Oleh:

Rezki Deritani
17/418661/PPA/05445

Serangan jaringan komputer dilakukan dengan berbagai cara untuk melumpuhkan pelayanan jaringan komputer tersebut, sehingga membahayakan pihak yang diserang. Keterlambatan peringatan serangan dapat berdampak fatal bagi kinerja *server*. Oleh karena itu dibutuhkan sebuah penerapan peringatan pada *snort* sebagai sarana komunikasi admin dan *server*.

Hal tersebut dapat dilakukan dengan menambahkan *instant messaging* sebagai media penghubung antara *snort* dengan admin. *Snort* merupakan sistem pendeteksi serangan yang memantau segala kegiatan ditrafik jaringan. *Snort* mengenali jenis serangan dengan memanfaatkan *rules*. Fungsi dari *rules* ialah untuk mengidentifikasi paket. Paket tersebut merupakan *log honeyd* yang digunakan sebagai acuan untuk *generated rules*.

Pembuatan *rules* pada *snort* membantu *snort* dalam mendeteksi serangan dan penambahan *instants messaging* pada *snort* menghasilkan notifikasi peringatan kewaspadaan apabila terjadi serangan kepada admin. Oleh karena itu dapat disimpulkan bahwa dengan adanya *generated rules*, serangan lebih mudah dikenali dan sistem peringatan dengan *instant messaging* membantu admin mengetahui terjadinya serangan pada *server*.

Kata Kunci: *Server, Instant messaging, Snort, Generate Rules, Log Honeyd*



ABSTRACT

EARLY WARNING OF COMPUTER NETWORKS BASED ON GENERATED RULES AND LOG HONEYD

By:

Rezki Deritani
17/418661/PPA/05445

Computer network attacks are carried out in various ways to disable the computer network services, thus endangering the party attacked. A delay in attack alerts can have a fatal impact on server performance. Therefore, we need a warning application in snort as a means of admin and server communication.

This can be done by adding instant messaging as a liaison between snort and admin. Snort is an attack detection system that monitors all network traffic activities. Snort recognizes the type of attack using rules. The function of the rules is to identify the package. The package is a honeyd log that is used as a reference for generated rules.

Making rules on snort helps snort in detecting attacks and adding instants messaging in snort generates alert notifications in case of an attack to the admin. Since it can be concluded that with the generated rules, attacks are more easily recognized and a warning system with instant messaging helps the admin know of an attack on the server.

Keyword: Server, Instant messaging, Snort, Generate Rules, Log Honeyd