

INTISARI

DESAIN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM DENGAN SNORT BERBASIS *DOCKER-CONTAINER*

Lorensius Oksigi

18/431569/SV/15540

Ancaman serangan jaringan merupakan isu serius yang dihadapi oleh setiap organisasi atau perusahaan. Serangan terhadap sistem atau *server* dapat menyebabkan *service* dari organisasi atau perusahaan terganggu. Untuk mencegah ancaman dari serangan jaringan dibutuhkan sistem yang mampu mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. *Intrusion Detection System (IDS)* adalah sistem perangkat lunak maupun perangkat keras yang bertugas mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan. Salah satu perangkat lunak yang bisa digunakan sebagai sistem IDS adalah snort. Snort adalah *software open-source* multi *operating system* yang dapat berjalan di OS linux, windows, BSD, solaris dan sistem operasi lainnya. Snort adalah *network-based* IDS yang menggunakan *signature-based detection* dan bekerja dengan cara menganalisis paket data yang lewat, apakah sesuai dengan jenis serangan yang sudah diketahui olehnya. Untuk m Docker perangkat lunak *open-source* untuk virtualisasi berbasis container untuk membangun, menguji dan menyebarkan aplikasi terdistribusi di lingkungan terisolasi. Pada penelitian kali ini akan dilakukan perancangan dan implementasi dinamis IDS menggunakan snort berbasis *docker-container*. IDS snort diimplementasikan dengan arsitektur docker untuk membangun sistem IDS yang hemat *memory*, *processor* dan *storage* serta ramah terhadap skalabilitas dan mudah terdistribusi dalam lingkungan yang terisolasi.

Kata kunci: ancaman serangan jaringan, *Intrusion Detection System (IDS)*, snort, docker

ABSTRACT

DESIGN AND IMPLEMENTATION DYNAMIC INTRUSION DETECTION SYSTEM (IDS) WITH SNORT BASED ON DOCKER-CONTAINER

Lorensius Oksigi

18/431569/SV/15540

The threat of network attacks is a serious issue faced by every organization or company. Attacks on a system or server can disrupt the services of the organization or company. To prevent threats from network attacks, a system is needed that can detect suspicious activity in a system or network. Intrusion Detection System (IDS) is a software or hardware system that is tasked with detecting suspicious activity in a system or network. One software that can be used as an IDS system is snort. Snort is an open-source software that can run on various operating systems such as Linux, Windows, BSD, Solaris, and other operating systems. Snort is a network-based IDS that uses signature-based detection and works by analyzing data packets that pass through it to determine if they match a known attack type. Docker is an open-source software for container-based virtualization used to build, test, and deploy distributed applications in isolated environments. In this study, a dynamic IDS design and implementation using snort based on docker-containers will be conducted. Snort IDS is implemented with a docker architecture to build an IDS system that is memory, processor, and storage efficient, as well as scalable and easily distributable in isolated environments.

Keywords: *Threat of network attacks, Intrusion Detection System (IDS), snort, docker*