INTISARI

IMPLEMENTASI *NETWORK DETECTION* DAN *PREVENTION SYSTEM* (NIDPS) BERBASIS SNORT DAN KIBANA DENGAN MENGGUNAKAN DOCKER CONTAINER

Mohammad Allaam Rasyaad Somardani

19/447095/SV/16814

Perubahan kehidupan masyarakat yang secara masif mulai bergerak terus mengadopsi teknologi dalam kegiatan sehari-hari, hal ini menimbulkan kekhawatiran dalam menjamin keamanan teknologi yang digunakan oleh masyarakat. Berbagai ancaman yang diketahui seperti *port scan*, *traffic flood attack* dan lain sebagainya menjadi ancaman penurunan layanan web dan kebocoran data. Kondisi ini mendorong keamanan pada bidang teknologi untuk terus meningkat dengan memanfaatkan dan mengolaborasikan berbagai teknologi yang sudah ada. Untuk terus mendukung kemajuan teknologi, khususnya pada bidang keamanan informasi dan jaringan, menggunakan docker container dan memadukannya dengan sistem pemantauan dan pencegahan serangan pada jaringan atau *Network Intrusion Detection and Prevention System* (NIDPS) dapat menjadi salah satu solusi untuk permasalahan dalam bidang keamanan. Saat ini docker sudah mulai banyak digunakan dalam instrumen teknologi informasi, docker dapat memudahkan *engineer* untuk saling mengembangkan proyek atau kebutuhan tanpa perlu mengkhawatirkan ketersediaan *dependencies* untuk mendukung pelaksanaan proyek tersebut. Karena itu penggunaan docker dalam menjalankan NIDPS dapat mempermudah proses instalasi keamanan jaringan. Snort dapat digunakan untuk menerapkan NIDPS ini untuk memantau jaringan, menyimpan hasil deteksi dan melakukan *drop packet* dari setiap ancaman. Percobaan pada penelitian ini snort IPS berhasil menjatuhkan 2168830 paket SYN *Flood*, 36771 paket ICMP *Flood* dan 90841 paket UDP *Flood*. Kibana dapat memudahkan untuk memantau dan menganalisis aktivitas dari snort NIDPS dengan teknologi *web monitoring* melalui *log* yang dihasilkan oleh snort.

Kata Kunci: keamanan jaringan, kibana, NIDPS, snort.

ABSTRACT

IMPLEMENTATION OF NETWORK DETECTION AND PREVENTION SYSTEM (NIDPS) USING DOCKER CONTAINER

Mohammad Allaam Rasyaad Somardani

19/447095/SV/16814

Massive changes in people's lives have started to move and continue to adopt technology in their daily activities, this has raised concerns in ensuring the security of the technology used by the community. Various known threats such as port scans, traffic flood attacks and so on are threats to web service degradation and data leaks. This condition encourages security in the field of technology to continue to improve by utilizing and collaborating with various existing technologies. To continue to support technological advances, especially in the field of information and network security, using the Docker container and integrating it with a network monitoring and attack prevention system or Network Intrusion Detection and Prevention System (NIDPS) can be a solution to problems in the security sector. Currently, Docker has begun to be widely used in information technology instruments, Docker can make it easier for engineers to develop projects or mutual needs without worrying about the availability of dependencies to support the implementation of the project. Therefore, using Docker to run NIDPS can simplify the process of installing network security. Snort can be used to implement this NIDPS to monitor the network, store detection results and drop packets of any threats. Attempts in this study snort IPS managed to drop 2168830 SYN Flood packets, 36771 ICMP Flood packets and 90841 UDP Flood packets. Kibana can make it easier to monitor and analyze the activities of snort NIDPS with web monitoring technology through logs generated by snort..

Keywords: kibana, NIDPS, network security, snort.