INTISARI

IMPLEMENTASI DAN ANALISIS INTRUSION DETECTION SYSTEM BERBASIS SURICATA PADA JARINGAN HOTSPOT MIKROTIK KAMPUNG WARUNGBOTO TERHADAP SERANGAN PORT SCANNING, DDOS, DAN BRUTE FORCE ATTACK

Internet telah menjadi kebutuhan setiap orang dalam berbagai aspek kehidupan dalam bermasyarakat di era ini. Dengan mengimplementasikan *hotspot* berbasis Mikrotik sebagai *gateway-server* pada suatu jaringan, masyarakat dapat mengakses jaringan internet untuk memenuhi kebutuhan daring secara praktis dan mudah. Implementasi *wifi access point* atau *hotspot* berbasis Mikrotik memudahkan masyarakat mengakses Internet untuk memenuhi kebutuhan akses informasi secara mudah. Mikrotik dilengkapi dengan fitur manajemen pengendalian akses dan *bandwidth* sehingga dapat membantu mengelola pemanfaatan Internet secara baik dan lancar. Namun, kemudahan akses jaringan melalui *hotspot* ini membuka peluang *hacker* untuk melancarkan serangan yang mengganggu atau meruak akses pengguna ke jaringan. Adapun resiko gangguan jaringan yang biasa dilakukan oleh *hacker* yaitu serangan *port scanning*, *Brute Force*, dan *DDoS attack*. Oleh karena itu penulis mengaplikasikan Sistem Deteksi Intrusi untuk medeteksi gangguan pada jaringan *hotspot* yang berbasis Suricata dengan menggunakan *platform* OPNSense. OPNsense merupakan platform atau operating system yang bersifat open source yang digunakan untuk memenuhi kebutuhan firewall dan Routing yang berbasis HardenendBSD. Atas dasar tersebut penulis mengimplementasikan Suricata IDS berbasis OPNSense dalam mendeteksi serangan jaringan berupa *Port Scanning*, *DDoS,* dan *Bruteforce* pada jaringan *hotspot* yang telah *terinstall* dan terdistribusi di kampung warungboto. Hasil pengujian diambil berdasarkan parameter yang diuji antara lain pengaruh penggunaan sumberdaya (cpu) pada *server* Mikrotik dan *server* IDS pada saat terjadi ketiga serangan tersebut, kemudian pengaruh besaran *traffict* data pengguna internet saat terjadi ketiga serangan tersebut, dan analisis hasil deteksi serangan pada IDS berdasarkan *log* dan *alert* yang ditampilkan.

Kata Kunci : *Suricata, IDS*, *OPNSense*, *Hotspot*, *Mikrotik, Port Scanning, DDoS*, *Brute Force Attack*.

ABSTRACT

IMPLEMENTATION AND ANALYSIS OF INTRUSION DETECTION SYSTEM BASED ON SURICATA ON MICROTIC HOTSPOT NETWORK WARUNGBOTO VILLAGE AGAINST PORT SCANNING, DDOS, AND BRUTE FORCE ATTACK ATTACKS

The internet has become a necessity for everyone in various aspects of life in society in this era. By implementing a Mikrotik-based *hotspot* as a network *gateway-server*, people can access the internet network to meet online needs practically and easily. The implementation of a Mikrotik-based *wifi access point* or *hotspot* makes it easier for people to access the Internet to meet their information access needs easily. Mikrotik is equipped with access and bandwidth control management features so that it can help manage Internet utilization properly and smoothly. However, the ease of network access through this hotspot opens up opportunities for *hackers* to launch attacks that disrupt or undermine user access to the network. The risk of network disturbances that are usually carried out by hackers are *port scanning* attacks, *Brute Force*, and *DDoS* attacks. Therefore, the authors apply the *Intrusion Detection System* to detect disturbances in the *Suricata-based hotspot* network using the OPNSense platform. OPNsense is an open source platform or operating system that is used to meet the needs of *HardenendBSD-based firewalls* and *routing*. On this basis, the author implements OPNSense-based Suricata IDS in detecting network attacks in the form of *Port Scanning*, *DDoS*, and *Bruteforce* on *hotspot* networks that have been installed and distributed in the warungboto village. The test results were taken based on the parameters tested, including the influence of resource usage (cpu) on the Mikrotik server and IDS server when the three attacks occurred, then the effect of the amount of internet user data traffic when the three attacks occurred, and analysis of the results of attack detection on IDS based on logs. and alerts are displayed.

Keywords: *Suricata, IDS, OPNSense, Hotspot, Mikrotik, Port Scanning, DDoS, Brute force Attack.*