ABSTRAK

IBNU RIKO RAMDANI. Analisis Serangan Web Server Menggunakan Wazuh dan Opnsense. Dibimbing oleh FERDI CHAHYADI dan NURUL HAYATY.

Keamanan web server merupakan aspek krtusial dalam menjaga integritas dan ketersediaan layanan digital di era saat ini. Menigkatkan ancaman siber menuntut implementasi solusi keamanan yang konprehensif untuk mendeteksi dan mencegah berbagai jenis serangan. Penelitian ini bertujuan untuk menganalisis efektivitas kombinasi wazuh sebagai sistem deteksi intrusi (IDS) berbasis *host* dan *Security Information and Event Management* (SIEM), serta OPNsense sebagai *firewall* dan *router* dalam melindungi web server dari serangan siber.

Metode penelitian yang digunakan meliputi identifikasi masalah, studi literatur, pembangunan lingkungan pengujian yang terdiri dari *dummy web server*, instalasi dan konfigurasi OPNsense, serta instalasi dan konfigurasi Wazuh. Selanjutnya, dilakukan simulasi berbagai jenis serangan terhadap *web server* yang dilindungi untuk menguji kemampuan Wazuh dalam mendeteksi anomali dan OPNsense dalam memblokir lalu lintas berbahaya. Hasil pengujian menunjukkan bahwa Wazuh berhasil mendeteksi berbagai pola serangan seperti *SQL Injection*, *Cross-Site Scripting* (XSS), *Brute Force*, dan *Denial of Service* (DoS) dengan akurat melalui analisis log dan aturan kustom. Sementara itu, OPNsense terbukti efektif dalam memblokir lalu lintas berbahaya pada *layer* jaringan dan aplikasi, mengurangi *surface attack web server*. Integrasi keduanya memberikan lapisan keamanan yang kuat, memungkinkan deteksi dini dan mitigasi serangan secara proaktif. Penelitian ini menyimpulkan bahwa kombinasi Wazuh dan OPNsense merupakan solusi yang efektif dan efisien untuk meningkatkan keamanan *web server* dari berbagai ancaman siber.

Kata kunci: *Web Server Security, Wazuh, OPNsense, Intrusion Detection System* (IDS), *Firewall*, Serangan siber.

ABSTRACT

IBNU RIKO RAMDANI. Analysis of Web Server Attacks Using Wazuh and OPNsense. Supervised by FERDI CHAHYADI dan NURUL HAYATY.

Web server security is a crucial aspect in maintaining the integrity and availability of digital services in the current era. The increasing cyber threats necessitate the implementation of comprehensive security solutions to detect and prevent various types of attacks. This research aims to analyze the effectiveness of combining Wazuh as a host-based Intrusion Detection System (IDS) and Security Information and Event Management (SIEM), and OPNsense as a firewall and router, in protecting a web server from cyber attacks.

The research methodology includes problem identification, literature review, building a test environment consisting of a dummy web server, OPNsense installation and configuration, and Wazuh installation and configuration. Subsequently, various types of attacks were simulated against the protected web server to test Wazuh's ability to detect anomalies and OPNsense's capability to block malicious traffic. The test results indicate that Wazuh successfully detected various attack patterns such as SQL Injection, Cross-Site Scripting (XSS), Brute Force, and Denial of Service (DoS) accurately through log analysis and custom rules. Meanwhile, OPNsense proved effective in blocking malicious traffic at the network and application layers, reducing the web server's attack surface. The integration of both provides a robust security layer, enabling early detection and proactive mitigation of attacks. This study concludes that the combination of Wazuh and OPNsense is an effective and efficient solution for enhancing web server security against various cyber threats.

Keywords: Web Server Security, Wazuh, OPNsense, Intrusion Detection System (IDS), Firewall, Cyber Attacks.