RANCANG BANGUN DAN ANALISIS SISTEM KEAMANAN JARINGAN MENGGUNAKAN WAZUH DAN T-POT DI PT GLOBAL INTERMEDIA NUSANTARA
Rangga Wiguna, Alif Subardono, ST.,M.Eng.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

RANCANG BANGUN DAN ANALISIS SISTEM KEAMANAN JARINGAN MENGGUNAKAN WAZUH DAN T-POT DI PT GLOBAL INTERMEDIA NUSANTARA

Perkembangan teknologi informasi yang semakin pesat menyebabkan meningkatnya ancaman keamanan jaringan terhadap server dan aplikasi web sehingga diperlukan sistem keamanan yang mampu melakukan deteksi, pemantauan, dan analisis serangan. Penelitian ini bertujuan untuk membangun sistem keamanan jaringan menggunakan Wazuh sebagai Security Information and Event Management (SIEM) dan Endpoint Detection and Response (EDR), serta T-Pot sebagai honeypot. Metode penelitian dilakukan dengan membangun lingkungan virtual menggunakan Proxmox sebagai target server dan Kali Linux sebagai mesin attacker. Pengujian dilakukan melalui simulasi serangan serta pengukuran delay pengiriman log dari rsyslog ke Wazuh untuk mengevaluasi kinerja sistem monitoring. Hasil penelitian menunjukkan bahwa sistem mampu mendeteksi aktivitas serangan melalui dashboard Wazuh, merekam aktivitas penyerang menggunakan T-Pot, serta menerima dan menganalisis log dari rsyslog dengan waktu pengiriman yang relatif singkat sehingga mendukung proses monitoring keamanan secara mendekati real-time. Implementasi sistem keamanan ini diharapkan dapat membantu administrator jaringan dalam meningkatkan kemampuan monitoring, analisis, dan mitigasi ancaman keamanan jaringan.

Kata Kunci: Wazuh, T-Pot, Keamanan Jaringan, Honeypot, SIEM.

UNIVERSITAS
GADJAH MADA
RANCANG BANGUN DAN ANALISIS SISTEM KEAMANAN JARINGAN MENGGUNAKAN WAZUH DAN T-POT DI PT GLOBAL INTERMEDIA NUSANTARA
Rangga Wiguna, Alif Subardono, ST.,M.Eng.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

DESIGN AND ANALYSIS OF A NETWORK SECURITY SYSTEM USING WAZUH AND T-POT AT PT GLOBAL INTERMEDIA NUSANTARA

The rapid advancement of information technology has led to an increasing number of cybersecurity threats targeting servers and web applications, making it essential to implement security systems capable of detecting, monitoring, and analyzing cyberattacks. This study aims to develop a network security system using Wazuh as a Security Information and Event Management (SIEM) platform and T-Pot as a honeypot. The research was conducted by building a virtual environment using Proxmox as the target server platform and Kali Linux as the attacker machine. The system was evaluated through simulated cyberattack scenarios and log transmission delay testing between rsyslog and Wazuh to assess the performance of the centralized monitoring system. The results show that the proposed system is capable of detecting attack activities through the Wazuh dashboard, recording attacker interactions using T-Pot, and receiving and analyzing logs forwarded by rsyslog with relatively low transmission delay, thereby supporting near real-time security monitoring. The implementation of this security system is expected to assist network administrators in improving monitoring, analysis, and mitigation capabilities against network security threats.

Keywords: *Wazuh, T-Pot, Network Security, Honeypot, SIEM.*