DETEKSI DINI SERANGAN SIBER PADA SISTEM INFORMASI AKADEMIK BERBASIS WEB MENGGUNAKAN *WAZUH*

Nama	: Fatullazi Abdul Haq
Nim	: 6404221112
Dosen Pembimbing 1	: Mansur, M.Kom
Dosen Pembimbing 2	: Nurmi Hidayasari, ST., M.Kom

ABSTRAK

Perkembangan teknologi informasi yang semakin maju dalam penggunaan sistem informasi berbasis web pada lingkungan Pendidikan, termasuk pada sistem informasi akademik yang mana, sistem berbasis web memiliki potensi kerentanan terhadap berbagai jenis serangan siber, seperti *Denial of Service* (DoS), *brute force*, dan *SQL Injection*. Oleh karena itu, diperlukan suatu sistem deteksi yang mampu memantau aktivitas sistem secara berkala dan memberikan peringatan terhadap potensi ancaman keamanan. Penelitian ini bertujuan untuk menerapkan sistem deteksi dini serangan siber pada website Jurusan Teknik Informatika Politeknik Negeri Bengkalis menggunakan platform Keamanan *Wazuh* yang terintegrasi dengan dashboard kustom SIEM dan notifikasi Telegram. Metode penelitian yang digunakan adalah dengan melakukan simulasi beberapa jenis serangan terhadap server website yang telah dipasang *Wazuh* Agent. Hasil penelitian menunjukan bahwa sistem *Wazuh* mampu mendeteksi berbagai jenis serangan yang dilakukan termasuk serangan DoS, *brute force*, dan *SQL Injection*. Setiap aktivitas serangan berhasil menghasilkan alert yang tercatat pada *Wazuh* Manager, ditampilkan pada dashboard Kustom SIEM, serta dikirimkan secara otomatis melalui notifikasi Telegram. Hal ini menunjukan hasil penelitian, sistem deteksi dini menggunakan *Wazuh* terbukti mampu mengidentifikasi serangan dan terintegrasi, sehigga dapat membantu administrator dalam melakukan Tindakan pencegahan lebih awal terhadap potensi ancaman keamanan sistem.

Kata Kunci: Deteksi dini, *Wazuh*, SIEM, serangan siber, sistem informasi akademik

EARLY DETECTION OF CYBER ATTACKS ON WEB-BASED ACADEMIC INFORMATION SYSTEMS USING WAZUH

Name	: Fatullazi Abdul Haq
Nim	: 6404221112
Supervisor 1	: Mansur, M.Kom
Supervisor 2	: Nurmi Hidayasari, ST., M.Kom

ABSTRACT

Advances in information technology have led to the increasing use of web-based information systems in education, including academic information systems. However, web-based systems are vulnerable to various types of cyber attacks, such as denial of service (DoS), brute force, and SQL injection. Therefore, a detection system is needed that can monitor system activity on a regular basis and provide warnings of potential security threats. This study aims to implement an early detection system for cyber attacks on the website of the Department of Informatics Engineering, Bengkalis State Polytechnic, using the Wazuh Security platform integrated with a custom SIEM dashboard and Telegram notifications. The research method used was to simulate several types of attacks on the website server that had been installed with Wazuh Agent. The results of the study show that the Wazuh system is capable of detecting various types of attacks, including DoS, brute force, and SQL injection attacks. Each attack activity successfully generated an alert that was recorded on Wazuh Manager, displayed on the Custom SIEM dashboard, and automatically sent via Telegram notification. This shows that research results indicate that the early detection system using Wazuh has proven capable of identifying attacks and is integrated, thereby assisting administrators in taking early preventive measures against potential system security threats.

Keywords: *Early detection, Wazuh, SIEM, cyber attacks, academic information systems*