

INTISARI

PROYEK AKHIR

ANALISIS PERFORMANSI WAZUH *END-POINT SECURITY HOST-BASED INTRUSION DETECTION SYSTEM* DALAM MENDETEKSI SERANGAN PADA SISTEM KOMPUTER USER DI PT. EMPORIA DIGITAL RAYA

Intrusion Detection System (IDS) merupakan sistem yang memiliki peran yang cukup penting dalam mendeteksi serangan pada suatu sistem. Wazuh *Host-based Intrusion Detection System* (HIDS) merupakan *Intrusion Detection System* (IDS) yang mampu mendeteksi ancaman yang terjadi, dengan cara mengenali pola seranganyang dilakukan oleh *Intruder*. Sistem tersebut diimplementasikan di PT Emporia Digital Raya pada seluruh sistem komputer yang ada untuk mendeteksi ancaman yang terjadi. Pada penelitian ini dilakukan analisis performansi pada Wazuh *server* dengan metode *All-in-One deployment* dan metode *Distributed deployment* dengan *docker container*. Hasil penelitian ini didapatkan bahwa nilai *response time* pada wazuh dengan metode *Distributed deployment* menggunakan *docker container* lebih rendah dibandingkan dengan metode *All-in-One deployment* dengan *docker container*, namun dari sisi penggunaan *resource* wazuh *server* dengan metode *All-in-One deployment* menggunakan *resource* yang lebih rendah dibandingkan dengan metode *Distributed deployment*.

Kata Kunci: *Security*, IDS, HIDS, Wazuh

ABSTRACT

Performance Analysis of Wazuh End-Point Security Host-Based Intrusion Detection System for Attacks Detection on User Computer System at PT. Emporia Digital Raya

Intrusion Detection System (IDS) is a system that has an important role in detecting attacks on a system. Wazuh Host-based Intrusion Detection System (HIDS) is an Intrusion Detection System (IDS) capable of detecting threats that occur, by recognizing patterns of attacks carried out by the Intruder. The system is implemented at PT Emporia Digital Raya on all existing computer systems to detect threats that occur. In this study, a performance analysis was carried out on the Wazuh server using the All-in-One deployment method and the Distributed deployment method with the docker container. The results of this study show that the response time value for the wazuh with the Distributed deployment method using the docker container is lower than the All-in-One deployment method with the docker container, but in terms of resource usage the wazuh server with the All-in-One deployment method uses different resources. lower than the Distributed deployment method.

Keywords: Security, IDS, HIDS, Wazuh