INTISARI

IMPLEMENTASI *FILE INTEGRITY MONITORING SYSTEM* MENGGUNAKAN *WAZUH OPEN SECURITY PLATFORM*

Aulia Khoirun Nisa
18/432056/SV/15992

Sistem audit dan monitor pada server merupakan hal yang penting pada suatu keamanan jaringan. Server biasanya digunakan untuk beban kerja yang cukup berat dan volume lalu lintas jaringan yang besar, sehingga dampaknya dapat menyebabkan waktu henti, informasi yang rusak, atau pelanggaran keamanan, yang semuanya dapat berdampak negatif. Dengan kebijakan audit yang telah ditentukan, administrator dapat melacak perubahan atau upaya untuk mengakses informasi penting yang telah terjadi pada server. Perubahan ataupun aktivitas tersebut perlu dilakukan monitor secara *real-time* ataupun berkala sehingga administrator bisa tahu dengan cara melihat perubahan apa saja yang terjadi, selain itu juga dapat mengidentifikasi tingat ancaman pada suatu server. *Wazuh platform* merupakan *software open source* yang digunakan untuk memonitor keamanan seperti *incident response*, *integrity monitoring, threat detection,*dan *compliance* dimana pada wazuh sendiri terdapat beberapa modul yang bisa digunakan untuk mendukung hal tersebut, salah satunya yaitu modul *File Integrity Monitoring (FIM)* yang dapat digunakan untuk memonitor direktori ataupun file pada sistem operasi. Pada sistem operasi Linux sendiri juga terdapat sistem audit yaitu *Audit Daemon* atau Auditd yang dapat digunakan untuk merekam peristiwa yang terjadi pada sistem Linux, dengan menggunakan *framework* ini sistem dapat melacak apa yang terjadi di sistem operasi dengan mendengarkan peristiwa berdasarkan aturan yang telah dikonfigurasi sebelumnya.

Kata kunci : Auditd, Wazuh, *Opensouce,File Integrity Monitoring*

ABSTRACT

IMPLEMENTATION OF FILE INTEGRITY MONITORING SYSTEM USING WAZUH OPEN SECURITY PLATFORM

Aulia Khoirun Nisa
18/432056/SV/15992

System audit and monitoring on the server are important in network security. Servers are typically used for moderately heavy workloads and large volumes of network traffic, so the impact can lead to downtime, corrupted information, or security breaches, all of which can have a negative impact. With predefined audit policies, administrators can track changes or attempts to access important information that has occurred on the server. These changes or activities need to be monitored in real-time or periodically so that administrators can know by looking at what changes have occurred, besides that they can also identify the level of threat on a server. The Wazuh platform is open-source software that is used to monitor security such as incident response, integrity monitoring, threat detection, and compliance where wazuh itself several modules can be used to support this, one of which is the File Integrity Monitoring (FIM) module which can be used to monitor directories or files on the operating system. In the Linux operating system itself, there is also an audit system, namely Audit Daemon or Auditd which can be used to record events that occur on Linux systems, using this framework the system can track what is happening in the operating system by listening to events based on previously configured rules.

Keywords: Auditd, Wazuh, Open source, File Integrity Monitoring