Implementasi Aplikasi Search and Reporting pada Security Information and Event Management Berbasis Splunk Enterprise untuk Sistem Deteksi Menggunakan Fitur Alerting Terhadap Data Serangan DoS = Implementation of Search and Reporting Application in Splunk Enterprise -Based Security Information and Event Management for Detection System Using Alerting Features for DOS Attack Data

Muhammad Alfiyansyah, author

Abstrak

Security Information and Event Management merupakan elemen penting dari keamanan suatu organisasi atau perusahaan yang dibutuhkan untuk monitoring secara real time serta melakukan analisis dari kejadian/event serta tracking dan logging dari data keamanan untuk keperluan audit data dan lain lain. Splunk adalah salah satu SIEM populer yang berbasis analitik yang mengumpulkan, menganalisis, dan menghubungkan volume trafik dari jaringan dan data mesin lainnya secara real time. Tujuan dari skripsi ini adalah untuk mengimplementasikan Splunk sebagai solusi SIEM terhadap ancaman serangan DoS yang disimulasikan dengan menggunakan aplikasi LOIC yang terpasang pada virtual machine penyerang yang memiliki sistem operasi Linux. Dengan ini diharapkan Splunk yang telah terpasang dapat melakukan monitoring, visualisasi data, serta menerapkan alert terhadap target yang diserang oleh serangan DoS. .....Security Information and Event Management is an important element of the security of an organization or company that is needed for real-time monitoring and analysis of events as well as tracking and logging of security data for data auditing and other purposes. Splunk is a popular analytics-based SIEM that collects, analyzes, and correlates traffic volumes from network and other machine data in real time. The purpose of this thesis is to implement Splunk as a SIEM against the threat of DoS attacks simulated by using the LOIC application installed on the attacker's virtual machine that has a Linux operating system. With this, it is expected that the installed Splunk can perform monitoring, data visualization, and apply alerts to targets attacked by DoS attacks.