Integrasi dan analisis snort intrusion detection system dengan interface web berbasis BASE pada sistem keamanan jaringan komputer = Integration and analysis of snort intrusion detection system with BASE-Based web interface on computer network security system

Fahmi Firman Ferdiansyah, author

Abstrak

IDS memerikan solusi keamanan jaringan yaitu dengan mendeteksi adanya akses ilegal atau penyusupan yang terjadi dalam jarigan komputer. Terdapat banyak jenis IDS yang didasarkan pada bagaimana administrator jaringan menerapkan IDS untuk mengamankan jaringan. Dalam penelitian ini Snort IDS akan diintegrasikan untuk dapat memberikan alerting maupun log apabila terjadi serangan di dalam jaringan, selain itu juga mampu melakukan monitoring serangan melalui interface web.
Sistem ini dibagi menjadi beberapa modul yaitu IDS software yaitu Snort, report modul yaitu BASE, dan juga Visual Syslog Server yang mampu mengirimkan alerting secara real time. Kinerja dari IDS yang telah diintegrasikan akan dianalisis dari penggunaan RAM dan CPU. Dengan Empat skenario penyusupan yang berbeda seperti IP Scanning, Port Scanning, DoS dan MitM dilakukan untuk melihat efeknya pada kinerja sistem.
Berdasarkan hasil pengujian yang telah dilakukan sistem berhasil mendeteksi adanya penyusupan dengan memberikan alert berdasarkan jenis serangan yang dilakukan. Pada penggunaan RAM dan CPU dapat terlihat adanya perbedaan ketika sistem mendeteksi adanya penyusupan pada jaringan. Penggunaan IDS yang telah diintegrasikan ini dapat menjadi langkah awal yang baik untuk mitigasi risiko pada jaringan dan sebagai peringatan awal adanya serangan cyber.
<hr>IDS describes network security solutions by detecting illegal access or intrusion that occurs in the computer network. There are many types of IDS based on how network administrators implement IDS to secure networks. In this study Snort IDS will be integrated to be able to provide alerts and logs if there is an attack on the network, besides that it is also capable of monitoring attacks through a web interface.
This system is divided into several modules those are IDS software (Snort), report module (BASE), and also Visual Syslog Server which is capable of sending alerts in real time. The performance of the IDS that has been integrated will be analyzed from the use of RAM and CPU. With four different intrusion scenarios such as IP Scanning, Portscanning, DoS, and MitM, it is done to see the effect on system performance.
Based on the results of testing, the system has successfully detected an inrusion by providing alerts based on the type of attack carried out. While the use of RAM and CPU can be seen a difference when the system detects an intrusion. The use of this integrated IDS can be a good first step to mitigate risk on the network and as an early warning of cyber attacks.