Implementasi dan analisa security information management menggunakan ossim pada sebuah perusahaan = Implementation and analysis of security information management in a company using ossim

Moehamad Rihal, author

Abstrak

Semakin banyak peralatan keamanan jaringan yang diimplementasikan, maka semakin banyak pula peralatan yang perlu dikelola dan dipantau. Semakin banyak peralatan yang dipasang maka semakin banyak log-log yang dihasilkan. Security Information Management (SIM) berfungsi menyediakan informasi yang terkait dengan keamanan jaringan secara terpusat.
Pada skripsi ini dimplementasikan sistem aplikasi security information management menggunakan OSSIM pada sebuah perusahaan dengan mengintegrasikan OSSIM dengan perangkat keamanan jaringan seperti IDP dan firewall. Pada skripsi ini juga dilakukan pemantauan terhadap trafik TCP, UDP dan ICMP selama satu pekan, dan melakukan skenario serangan ICMP flooding ke server OSSIM selama beberapa menit kemudian dianalisis kondisi jaringan pada hari tersebut.
Rata-rata trafik protokol baik TCP, UDP dan ICMP selama satu minggu menunjukkan bahwa pada saat jam kerja lebih tinggi dibandingkan pada saat bukan jam kerja. Rata-rata trafik TCP pada jam kerja lebih besar 74,85 kb (12,1 %), rata-rata trafik UDP lebih besar 50,6 kb/s (54,1 %) dan rata-rata trafik ICMP pada jam kerja lebih besar 19,1 b/s (7,6 %). Melalui skenario serangan Ping flooding ICMP ke server OSSIM menunjukkan bahwa OSSIM dapat mendeteksi serangan secara real-time melalui pengamatan trafik jaringan dan laporan SIEM event.
<hr>The more devices implemented in network security, the more devices are needed to be managed and monitored. Security Information Management (SIM) provides information which is related to centered security network.
In this final project, it has been implemented a SIM application system in a company by integrating OSSIM with security network devices such as IDP and firewall. Traffic monitoring for TCP, UDP and ICMP has been conducted for a week. An attacking scenario with ICMP flooding to OSSIM server has also been conducted for a few minutes and then the network condition for that day are analyzed.
The average of the traffic protocol of TCP, UDP and ICMP in a week are higher in the working hour than non-working hour. The average of TCP traffic at the working hour greater than 74.85 kb/s (12.1 %), UDP greater than 50.6 kb/s (54.1 %) and for ICMP greater than 19.1 b/s (7.6 %). From the flooding attack scenario, OSSIM can detect the attacking in real-time through the traffic monitoring and SIEM event report.