Analisis host based intrusion detection system menggunakan OSSEC = Analysis of host based intrusion detection system using OSSEC

Mohamad Widya Iswara, author

Abstrak

Jaringan komputer sangat berguna dalam pekerjaan manusia diantaranya dalam saling berkomunikasi satu sama lain. Oleh karena itu dibutuhkan keamanan jaringan yang berguna dapat menjaga kerahasiaan informasi dan juga menghindari serangan-serangan yang menimbulkan dampak negatif.
Pada skripsi ini akan dibahas mengenai bagaimana pengujian dan analisis dalam salah satu tools IDS (Intrusion Detection System) berbasis host atau yang biasa disebut HIDS (Host-Based Intrusion Detection System). HIDS yang digunakan adalah OSSEC karena bersifat Open Source. Pengujian ini bertujuan untuk mencari tahu keberhasilan, response time dan pengaruh OSSEC terhadap performansi jaringan melalui throughput yang didapat. Juga membandingkan OSSEC dengan Suricata dan Honeyd. Hasil dari pengujian terhadap functional test, OSSEC mampu mendeteksi serangan berupa port scanning dan SSHD brute force attack. Pada perhitungan response time, dihitung berdasarkan fitur OSSEC sebagaimana active-response yang mampu memutuskan koneksi terhadap IP penyerang dan response time yang didapat sebesar 2.1397618 detik. Juga OSSEC tidak mempunyai pengaruh yang besar pada performansi jaringan.
.....
Computer network is very useful in work beings communicate with each other. Therefore network security is needed which will keep the secret of information and also avoid the attacks that inflict a negative impact. At this final project will discuss about how to test and analysis of one of the IDS (Intrusion Detection System) tools based on host or commonly called HIDS (Host-Based Intrusion Detection System). And HIDS used is OSSEC because it is open source. This test aims to find out the success of OSSEC, response time and influence ossec againt network performance through throughput obtained. Also compare ossec with suricata and honeyd. Results from testing of the functional test, OSSEC is able to detect port scanning attack and SSHD brute force attack. On the calculation of response time, calculated based on the features OSSEC as active-response capable of disconnecting against the attacker's IP and response time obtained is 2.1397618 seconds. Also OSSEC have no great influence on network performance.