Analisis kinerja open source Intrusion Prevention System (IPS) terhadap serangan Denial of Service (DoS) pada sistem operasi Windows 10 = Performance analysis of open source Intrusion Prevention System (IPS) against Denial of Service (DoS) attacks on Windows 10 operating systems

Fadhilah Rheza Putranto, author

Abstrak

Pada setiap jaringan, selalu ada ancaman yang mengkompromasikan keamanan dan user.Salah satu ancaman ini adalah serangan Denial of Service (DoS attack). Serangan Denial of Service adalah serangan yang mematikan layanan dan jaringan, tidak dapat diakses oleh user. Serangan DoS dilakukan dengan flooding target dengan traffic, atau mengirimkannya informasi yang menyebabkan system crash. Salah satu metode yang dapat digunakan untuk mencegah serangan ini adalah dengan menggunakan Intrusion Prevention System (IPS). Sistem Pencegahan Intrusi yang berfungsi untuk menjaga keamanan jaringan dengan pencegahan dan mencegah ancaman atau serangan yang terindentifikasi. Intrusion Prevention System bekerja dengan jaringan user, mencari kemungkinan eksploit dan mendapatkan informasinya. Intrusion Prevention System memberikan informasi eksploit ini ke administrator sistem dan mengambil tindakan pencegahan, seperti menutup access point Pada penelitian ini dilakukan percobaan penyerangan seperti UDP flood attack, TCP flood attack, dan ICMP flood attack. Setelah itu dilakukan analisa performa menggunakan 2 open source IPS yaitu: Snort dan Suricata.dengan menganalisa efektivitas mereka. Dari serangan tersebut akan dilakukan analisis performansi IPS dan perhitungan security metric dengan metode VEA-bility. Hasil dari VEA-bility berupa nilai 0 hingga 10 yang diperoleh dari perhitungan nilai vulnerability dimension, exploitability dimension dan attackbility dimension akan menentukan tingkat keamanan sistem. Hasil dari analisis VEA-bility metric menunjukkan bahwa Suricata lebih “viable” dibangdingkan Snort.
.....On every network, there are always threats that compromise security and users. One of these threats is a Denial of Service attack (DoS attack). Denial of Service attacks are attacks that kill services and networks, inaccessible to the user. DoS attacks are performed by flooding the target with traffic, or sending it information that causes the system to crash. One method that can be used to prevent this attack is to use the Intrusion Prevention System (IPS). Intrusion Prevention System which functions to maintain network security by preventing and preventing identified threats or attacks. The Intrusion Prevention System works with a network of users, looking for possible exploits and getting their information. Intrusion Prevention System provides information on this exploit to system administrators and takes preventive action, such as closing the access point. In this study, attack trials such as UDP flood attack, TCP flood attack, dan ICMP flood attack were carried out. After that, performance analysis was carried out using 2 open source IPS, namely: Snort and Suricata by analyzing their effectiveness . From this attack, an IPS performance analysis will be carried out and the calculation of security metrics using the VEA-ability method. The results of VEA- ability in the form of values from 0 to 10 obtained from the calculation of the value of the vulnerability dimension, the exploitability dimension and the attackbility dimension will determine the level of system security. The results of the VEA-bility metric analysis show that Suricata is more viable than Snort.