Analisa melanisme pertahanan DOS dan DDOS (distributed denial of service) pada virtual machine dengan menggunakan IDS center = DoS and DDoS (distributed denial of service) defense mechanism analisys on the virtual machine using IDS center

Muhamad Zamrudi AH, author

Abstrak

Skripsi ini adalah sebuah analisa pada mekanisme pertahanan terhadap serangan Denial of Service dan Distributed Denial of Service. DoS dan DdoS adalah serangan yang sering terjadi dijaringan internet maupun jaringan lokal. Serangan ini berdampak negatif yang cukup merugikan korbannya. Serangan ini terbagi menjadi 2 yaitu logical dan flooding. Flooding merupakan jenis serangan yang sering terjadi. Maka dari itu akan perlu sebuah mekanisme pertahanan yang mampu menangani jenis serangan ini.
Pada skripsi ini dijelaskan tentang mekanisme pertahanan yang telah dibuat sedemikian rupa sehingga mampu diimplementasikan pada applikasi IDS center 1.1 dan Snort 2.8. Ujicoba dilakukan pada jaringan virtual yang dibuat menggunakan aplikasi VirtualBox. Aplikasi ini mampu membuat virtual machine yang dapat di-install Operating System. Dengan menggunakan jaringan virtual analisa dapat dilakukan lebih mudah. Simulasi serangan dilakukan menggunakan applikasi WinArpAttacker. WinArpAttacker adalah applikasi yang mampu membanjiri jaringan dengan paket tcp, arp maupun udp.
Analisa yang dilakukan dengan membandingkan parameter-parameter. Parameter tersebut antara lain adalah reliability dan response time. Parameter reliability mewakili tingkat keberhasilan mekanisme pertahanan pada percobaan yang dilakukan. Parameter response time mewakili tingkat delay dan waktu respon terhadap jaringan internet ketika terjadi serangan. Dari percobaan tersebut menghasilkan tingkat reliability ketika terjadi serangan DoS adalah 92% sedangkan pada DDoS adalah 82%. Nilai rata-rata response time terhadap jaringan internet per satuan waktu adalah 2086.75 ms.
<hr><i>This thesis is an analysis of the defense mechanisms against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. DoS and DDoS attacks often happen in Internetwork or local network. This attack is quite a negative impact against the victim. This attack is divided into 2 kinds which is logical and flooding. Flooding is a type of frequent attacks. Thus it would need a defense mechanism that can handle this type of attack.
In this thesis described the defense mechanisms that have been made in such a way that can be implemented in the application IDS 1.1 center and Snort 2.8. Test performed on a virtual network created using VirtualBox application. This application is able to create a virtual machine that can be installed operating system. By using a virtual network, analysis can be done more easily. Attack simulation conducted using WinArpAttacker 3.50 application. WinArpAttacker is an application that can flood the network with TCP, ARP or UDP packet.
The analysis carried out by comparing the parameters. These parameters include reliability and response time. Reliability parameter represents the uccess rate of defense mechanisms in the experiments conducted. This parameter represents the level of response time delay and response time of the Internet network during the attack. From the experimental results in the level of reliability when there is a DoS attack at 92% while DDoS is 82%. The average value of response time on the internet network per unit time was 2086.75

ms.</i>