DANALISA PROSES KILL BOTS DALAM MEMPERTAHANKAN DARI SERANGAN DISTRIBUTED DENIAL OF SERVICE DENGAN MENGGUNAKAN STRUKTUR DATA BLOOM FILTER

Ian Febrian Reza Mulia Yulianto
209115870

ABSTRAK

Distributed Denial of Service atau DDoS adalah salah satu serangan yang mengancam sekuritas dari server. Serangan tersebut mempunyai jenis yang beraneka ragam, contohnya adalah Flash Crowd. Serangan Flash Crowd adalah serangan yang mengandalkan banyaknya agent untuk mengakses server yang ingin diserang dan tidak adanya eksploitasi dari segi protokol maupun dari segi port yang ada. Flash Crowd mempunyai perilaku hampir sama seperti pengguna pada umumnya, dengan demikian penanganannya harus berdasarkan perilaku dari pengguna yang sebenarnya. Berdasarkan masalah tersebut terciptalah Kill Bots, sistem pertahanan terhadap serangan Flash Crowd. Pada tugas akhir ini, Kill Bots akan dianalisa dan diimplementasi ulang pada Apache web server dengan rupa modul Apache.

Kill Bots mempunyai dua buah status yang menandakan kondisi dari server saat itu, yaitu NORMAL dan SUSPECTED. Kill Bots memulai proses pembedaan antara pengguna yang sah dengan zombie dimulai pada kondisi server mencapai status SUSPECTED, di mana kondisi server pada saat itu mempunyai load server lebih dari 70%. Proses pembedaan atau autentikasi yang berjalan dengan menggunakan bantuan captcha dilakukan pada semua request yang baru masuk pada saat status SUSPECTED. Perilaku yang diharuskan untuk menjawab sebuah tes akan membedakan apakah itu pengguna yang sah atau tidak. Perilaku request yang berbau zombie, maka akan dimasukkan pada sebuah tabel zombie yang bersifat temporer. Ketika request yang telah dikenali sebagai zombie masuk, maka server akan langsung memberikan nilai kembalian bahwa request tersebut tidak dapat melanjutkan requestnya.

Pengujian yang dilakukan adalah pengujian performa antara tiga kondisi pertahanan dari server. Hasil dari pengujian performa akan disajikan dalam bentuk grafik garis di mana nilai yang ditunjukkan adalah nilai respond time dari server tanpa pertahanan apa pun, server dengan pertahanan mod_evasive, dan server dengan pertahanan Kil Bots.

ANALYSIS OF KILL BOTS PROCESS IN DEFENDING FROM DISTRIBUTED DENIAL OF SERVICE ATTACK USING BLOOM FILTER DATA STRUCTURE

Ian Febrian Reza Mulia Yulianto
209115870

ABSTRACT

DDoS is an attack that threaten the security of a server. It has many kind of variation, one of them is the Flash Crowd. Flash Crowd is an attack that relies on the number of agent for attacking the server and no exploitation on the protocol and port. Flash Crowd's behavior is similar to a normal user so the handling has to be based on a real user. This problem leads to the creation of Kill Bots, a defense system for the Flash Crowd. In this final project, Kill Bots will be analyzed and implemented on Apache web server using Apache module.

Kill Bots has two kind of status showing the server's condition, NORMAL and SUSPECTED. Kill Bots will start the separation of a normal user and a zombie when the server status is SUSPECTED (a condition where the server's load is more than 70%). The separation process (also known as the authentication process) that use the captcha is applied to all coming requests when the status is SUSPECTED. Behavior shown by the requests will differentiate between a real user and a zombie. Zombie users will be put in a temporary zombie table and the server will return a value result that the request can't proceed with its request.

The examination performed is a performance examination between three server conditions. The result of the examination will be shown by using the line chart where the value shown represents respond time from three kind of server : server without a defense system, server with mod_evasive defense system and server with Kill Bots defense system.