PERANCANGAN *BOT* UNTUK *MONITORING* SERVER DARI SERANGAN *DISTRIBUTED DENIAL OF SERVICE* MENGGUNAKAN *JSON WEB TOKEN*

ARIF MAULANA RAHMAN

ABSTRAK

Dalam menjalankan sebuah server diperlukan sistem *monitoring* untuk mengamankan jaringan agar meminimalisir resiko jika terjadi percobaan intrusi. Salah satu serangan yang sering terjadi kepada server merupakan serangan *DDOS* (*Distributed Denial of Service*) yang mengakibatkan sistem yang diserang mengalami gangguan berupa *error request*, *halt*, kegagalan sistem dan sebagainya. Berdasarkan permasalahan yang dijelaskan, maka diperlukan sebuah *bot* untuk melakukan *monitoring* serta melindungi server dari serangan *DDOS*, dalam penelitian ini difokuskan serangan *DDOS* yang berjenis *UDP Flooding* dan *SYN Flooding*. *Bot* ini akan mampu mendeteksi serangan *UDP Flooding* dan *SYN Flooding* dengan membatasi jumlah paket yang ditujukan kepada *port* yang dibuka oleh server, apabila *bot* mendeteksi serangan maka *bot* akan memblokir serta mengirimkan notifikasi kepada admin server dengan menerapkan *set push notification* serta menggunakan *JSON Web Token* untuk memastikan notifikasi yang dikirimkan oleh *bot* kepada *smartphone* admin server terjaga integritas dan kerahasiaannya. *Monitoring* server memanfaatkan *bot* untuk mendeteksi serangan *DDOS* berjenis *UDP Flooding* dan *SYN Flooding* dengan membatasi jumlah paket yang dikirimkan kepada *port* yang dibuka oleh server, apabila jumlah paket yang dikirimkan lebih dari 100 paket per detik maka *bot* akan mengidentifikasi pengiriman tersebut sebagai serangan. Penerapan metode *JSON Web Token* agar bisa dioperasikan oleh *bot* admin server yakni dengan mengimplementasikan *package JSON Web Token* pada *bot* lalu memanggil fungsi *encode* agar *JSON Web Token* dapat melakukan enkripsi pada klaim yang berisikan data penyerang oleh *bot*, sehingga *bot* admin server dapat mengamankan klaim yang akan dikirimkan ke admin server.

Kata Kunci: Keamanan, Jaringan, Server, Administrator, *Monitoring*, *Distributed Denial of Service*, *Bot*, *UDP Flooding, SYN Flooding, JSON Web Token*.

BOT DESIGN FOR SERVER MONITORING FROM DISTRIBUTED DENIAL OF SERVICE ATTACKS USING JSON WEB TOKEN

ARIF MAULANA RAHMAN

ABSTRACT

In running a server, a monitoring system is needed to secure the network in order to minimize the risk if an intrusion attempt occurs. One of the attacks that often occurs to servers is a DDOS (Distributed Denial of Service) attack which results in the system being attacked experiencing interference in the form of error requests, halt, system failure and so on. Based on the problems described, a bot is needed to monitor and protect the server from DDOS attacks, in this study the focus is on DDOS attacks of the UDP Flooding and SYN Flooding types. This bot will be able to detect UDP Flooding and SYN Flooding attacks by limiting the number of packets addressed to the port opened by the server, if the bot detects an attack the bot will block and send notifications to the server admin by implementing push notification sets and using JSON Web Tokens to ensure The integrity and confidentiality of notifications sent by the bot to the server admin smartphone are maintained. Server monitoring makes use of bot to detect DDOS attacks of the UDP Flooding and SYN Flooding types by limiting the number of packets sent to the port opened by the server, if the number of packets sent is more than 100 packets per second, the bot will identify the sending as an attack. The application of the JSON Web Token method so that it can be operated by the server admin bot, namely by implementing the JSON Web Token package on the bot and then calling the encode function so that the JSON Web Token can encrypt claims containing attacker data by bot, so that the admin server bot can secure claims that will sent to the server admin.

Keywords: *Security, Network, Server, Administrator, Monitoring, Distributed Denial of Service, Bot, UDP Flooding, SYN Flooding, JSON Web Token.*