Sistem Pendistribusian *Blacklisted IP* untuk Menangani Serangan DDoS pada Snort IPS berbasis Blockchain

Bram Andika Ahmad Al'aziz[1], Parman Sukarno[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]andikabram@student.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id

Abstrak

Serangan *Distributed Denial of Service* (DDoS) merupakan ancaman keamanan utama terhadap jaringan komputer dan penyedia layanan hingga saat ini. Serangan DDoS bekerja dengan membuat suatu layanan menjadi berhenti dan tidak dapat diakses. Skema mitigasi serangan DDoS yang ada saat ini memiliki kekurangan karena kurangnya fleksibilitas dan memerlukan biaya yang tinggi. Teknologi terbaru seperti blockchain memungkinkan untuk mengatasi masalah tersebut dengan cara terdistribusi sehingga beban mitigasi dapat berkurang dengan biaya yang cukup rendah. Melalui *smart contract* yang ada pada ethereum blockchain memungkinkan untuk menginformasikan sumber serangan atau *blacklisted IP* (*Internet Protocol*) tanpa memerlukan tambahan infrastruktur. *Blacklisted IP* digunakan oleh *Intrusion Prevention System* (IPS) untuk mendeteksi dan menangani serangan DDoS. IPS merupakan sebuah sistem yang digunakan untuk melakukan pendeteksian dan penanganan terhadap serangan pada jaringan komputer. Dalam penelitian ini diusulkan mekanisme pendistribusian informasi sumber serangan dengan cara menggabungkan teknologi blockchain dengan IPS sehingga mitigasi serangan DDoS menjadi lebih fleksibel dan hemat biaya. Skema yang diajukan tersebut merupakan mekanisme keamanan tambahan untuk sistem penanganan serangan DDoS yang sudah ada, tanpa perlu membuat daftar sumber serangan khusus dan mekanisme pendistribusian lainnya. Melalui skema pendistribusian tersebut dilakukan pengujian dan analisis untuk melihat informasi sumber serangan pada setiap IPS dan lalu lintas serangan yang lewat pada jaringan. Hasilnya adalah setiap IPS dapat memiliki informasi sumber serangan yang sama dan lalu lintas serangan yang melalui infrastruktur jaringan dapat berkurang.

Kata kunci : DDoS, IPS, Blockchain, Blacklisted IP, Smart Contract.

Abstract

Distributed Denial of Service (DDoS) attacks are a major security threat to computer networks and service providers until now. DDoS attacks work by making a service stop and inaccessible. The current DDoS attack mitigation scheme has shortcomings due to lack of flexibility and requires high costs. The latest technologies such as blockchain make it possible to overcome these problems in a distributed manner so that the burden of mitigation can be reduced at a fairly low cost. Through the smart contract in the ethereum blockchain it is possible to inform the source of the attack or blacklisted IP (Internet Protocol) without the need for additional infrastructure. Blacklisted IP is used by Intrusion Prevention System (IPS) to detect and handle DDoS attacks. IPS is a system that is used to detect and handle attacks on computer networks. In this research, it is proposed the mechanism for distributing information on the source of attacks by combining blockchain technology with IPS so that the mitigation of DDoS attacks becomes more flexible, and cost-effective. The proposed scheme is an additional security mechanism for handling DDoS systems that already exist, without the need to make a list of special attack sources and other distribution mechanisms. Through the distribution scheme, testing and analysis are carried out to see the source of attack information on each IPS and attack traffic that passes on the network. The result is that each IPS can have the same source of attack information and attack traffic through the network infrastructure can be reduced.

Keywords: DDoS, IPS, Blockchain, Blacklisted IP, Smart Contract.