

INTISARI

DETEKSI DAN MITIGASI SERANGAN DDOS PADA *SOFTWARE DEFINED NETWORK* MENGGUNAKAN SNORT DAN *PACKET FILTERING IPTABLES*

Dheni Yulia Dinda Pratiwi

19/447088/SV/16807

Software Defined Network (SDN) merupakan pendekatan dalam pengelolaan jaringan yang memisahkan lapisan kontrol (*control plane*) dan lapisan pengiriman (*data plane*) dalam jaringan. Pada jaringan SDN, *control plane* dikendalikan secara sentral melalui perangkat lunak yang disebut "*controller*", sementara *data plane* terdiri dari perangkat jaringan fisik seperti *switch* dan *router*. Akan tetapi, pemisahan ini menimbulkan banyak masalah keamanan. Oleh karena itu, kebutuhan untuk melindungi jaringan dari berbagai serangan menjadi hal yang wajib dilakukan. *Distributed Denial of Service* (DDoS) adalah salah satu serangan yang menjadi rintangan bagi pengguna SDN. Upaya melindungi jaringan SDN dari serangan DDoS diperlukan sebuah sistem yang dapat mendeteksi dan mencegah serangan tersebut. Pada tugas akhir ini, dibuat sebuah sistem yang digunakan untuk mendeteksi adanya serangan DDOS dengan menggunakan Snort IDS (*Intrusion Detection System*) dan pencegahannya dengan implementasi *firewall* pada server dengan menggunakan Iptables. Jika DDOS terdeteksi, informasi penyerang akan ditampilkan dalam *log* Snort IDS dan paket akan diblok oleh *firewall* server.

Kata kunci : *Software Defined Network, DDoS, Snort, Iptables.*

ABSTRACT

DETECTION AND MITIGATION OF DDOS ATTACK IN SOFTWARE DEFINED NETWORK USING SNORT AND PACKET FILTERING – IPTABLES

Dheni Yulia Dinda Pratiwi

19/447088/SV/16807

Software-Defined Networking (SDN) is an approach to network management that separates the control plane from the data plane of the network. In an SDN network, the control plane is centrally controlled by software called a "controller," while the data plane consists of physical network devices such as switches and routers. However, this separation creates many security issues. Therefore, it is imperative to protect the network from various attacks. Distributed Denial of Service (DDoS) is one such attack that poses a hurdle for SDN users. Efforts to protect the SDN network from DDoS attacks require a system that can detect and prevent these attacks. In this final project, a system is created that detects DDOS attacks using Snort IDS (Intrusion Detection System) and prevents them by implementing a firewall on the server using Iptables. When DDOS is detected, attacker information is displayed in Snort IDS logs and packets are blocked by the server firewall.

Keywords: Software Defined Network, DDoS, Snort, Iptables.