ABSTRAK

Keamanan merupakan hal penting pada sebuah jaringan komputer. Dengan makin berkembangnya komputasi berbasis awan, ancaman keamanan pada jaringan tersebut juga ikut berkembang. Hasil survey dari *Cloud Security Alliance* (CSA), menyatakan bahwa di antara semua masalah keamanan jaringan, penyalahgunaan dari komputasi awan merupakan salah satu ancaman terbesar, dengan mudahnya *hackers* menyalahgunakan sistem komputasi awan untuk melancarkan serangan terhadap jaringan. Dari banyaknya jenis serangan terhadap jaringan berbasis awan, salah satu yang paling terkenal adalah serangan botnet. Botnet dapat digunakan untuk berbagai macam tujuan, seperti *Spamming*, *BruteForcing*, dan serangan DoS.

Openflow merupakan implementasi dari konsep SDN. Openflow merupakan standarisasi yang mendefinisikan antarmuka sistem komunikasi antara *control plane* dan *data plane* pada arsitektur SDN. Pada penelitian ini dijelaskan bagaimana openflow dibangun dan digunakan sebagai alat pendeteksi adanya intrusi pada jaringan komputasi awan, khususnya jenis serangan DoS yang dilakukan pada jaringan komputasi awan. Penulis menggunakan Open VSwitch sebagai switch virtual pada server, ryu sebagai kontroler pada jaringan berbasis openflow, dan snort sebagai alat pendeteksi adanya serangan pada jaringan komputasi awan.

Kata kunci: SDN, OpenFlow, ryu, snort, NIDS, DoS

ABSTRACT

Security system is definitely one of the most crucial part on a computer network. As the concept of cloud computing continues to grow, threats and severity of cyber-attacks have also grown day by day. The survey that conducted by Cloud Security Alliance (CSA) has stated, on all of the threats on computer network, cloud-based network has the biggest horrific cases of cybercrimes related to massive data breaches, flaws in microchips, cryptojacking, and many others. Among various network attacks, botnet led attacks are considered as the most serious threats. A botnet, i.e., the network of compromised computers is able to perform large scale illegal activities such as Distributed Denial of Service attacks, Spamming, BruteForcing, etc.

Openflow is considered one of the first software-defined networking (SDN) standards. Openflow separates the programming of routers and switches from underlying hardware. This paper explained on how Open VSwitch, Ryu Controller, and snort are collaborated to make an openflow-based network that is constructed and used as cloud-based network intrusion detection system.

Keywords: SDN, OpenFlow, ryu, snort, NIDS, DoS