Implementasi dan analisis keamanan software defined network controller floodlight, ONOS, dan Ryu terhadap serangan control message abuse dan CPU exhaustion menggunakan framework DELTA = Implementation and security analysis of Floodlight, ONOS, and Ryu software defined netwrok controller against control message abuse and CPU exhaustion attacks using DELTA framework

Wisnu Wicaksono, author

Abstrak

ABSTRAK
Software Defined Network (SDN) adalah suatu arsitektur baru dalam jaringan komputer. SDN dirancang dengan pendekatan berupa pemisahan antara lapisan kontrol (control plane) dan lapisan penerus (forwarding plane). Arsitektur SDN bertujuan agar manajemen jaringan lebih dinamis dan mampu beradaptasi dengan traffic yang besar. Meski begitu isu keamanan menjadi permasalahan tersendiri dalam implementasinya. Controller yang terspusat menjadi titik yang banyak memiliki celah keamanan. Berbagai controller SDN dikembangkan oleh vendor jaringan dengan karakteristik dan environment yang berbeda-beda. Oleh karena itu dalam pengujian keamanan suatu controller diperlukan lingkukan uji yang khusus bergantung pada controller yang dipakai. Dalam penelitian ini analisis keamanan SDN dilakukan menggunakan alat automasi berupa framework berbasis open source. Berbagai lingkungan uji dan skenario serangan tertentu pada beberapa controller dapat dilakukan menggunakan framework ini. Pada penelitian ini dilakukan empat skenario serangan yaitu Flow Rule Flooding, CPU Exhaustion, Flow Table Clearance, dan Flow Rule Modification. Masing-masing serangan diujikan pada controller Floodlight, ONOS, dan Ryu. Floodlight dan ONOS dapat mengatasi skenario serangan Flow Rule Flooding, dan CPU Exhaustion namun tidak dapat mengatasi serangan Flow Table Celarance dan Flow Rule Modification. Sedangakan Ryu tidak dapat mengatasi keempat serangan tersebut. <hr />
<hr>
ABSTRACT
Software Defined Network (SDN) is a new architecture in computer networks. SDN is designed with an approach in the form of separation between the control layer and forwarding layer. SDN architecture aims to make network management more dynamic and able to adapt to large traffic. Even so, security issues become a separate problem in their implementation. The centralized controller becomes a point that have many vulnerabilities. Various SDN controllers are developed by network vendors with different characteristics and environments. Therefore, in testing the security of a controller, a special test environment is needed depending on the specific controller. In this study, SDN security analysis is done using an automation tool in the form of an open source based framework. Various test environments and certain attack scenarios on some controllers can be done using this framework. In this study four attack scenarios were carried out, they are Flow Rule Flooding, CPU Exhaustion, Flow Table Clearance, and Flow

Rule Modification. Each attack is tested on the Floodlight, ONOS, and Ryu controllers. Floodlight and ONOS can overcome the scenario of Flow Rule Flooding, and CPU Exhaustion. While Ryu cannot overcome the four attacks.