ABSTRACT

Attacks on network infrastructure are a serious challenge that needs to be addressed. In this study, we developed an automated mitigation system based on Software Defined Networking (SDN) that combines snort IDS, Ryu Controller and Open vSwitch (OVS) to detect and block suspicious traffic in real time. This system works by monitoring logs from snort, then extracting suspicious source IPs and sending them to the SDN Ryu controller for processing. Furthermore, the rules are sent to OVS so that malicious traffic can be stopped. Based on the test results, the system is able to actively block malicious traffic, resulting in a packet loss of 98% on the attacker side. Proving that the designed automated mitigation system is effective and able to improve the security system on the network without requiring manual intervention.

Keywords: Software Defined Networking (SDN), Ryu Controller, Snort IDS, Open vSwitch (OVS)