ABSTRACT

SDN *is one of the innovations resulting from technological developments. The technology in SDN provides a control plane that is complete and separate from the data plane. This separation also makes* SDN *a combined function of forwarding data packets and routing processes on this network. This separation is one of the gaps that is a weakness in* SDN. *One of the weaknesses found in* SDN *is its vulnerability to security attacks. Researchers use this vulnerability to find out the mechanism of the* MITM *attack on* SDN.

MITM *is an attack with an attack concept where the attacker becomes a third party in the middle of the target to intercept information on data packet traffic. The purpose of this eavesdropping is to obtain sensitive information that passes between targets. This* MITM *attack is carried out in 2 stages, namely the Interception stage and the Decryption stage. One of the tools for performing* MITM *attacks is* Ettercap.

Ettercap *has many executable features to support* MITM *attacks. The attack scenario carried out in this study is by simulating using different features that can be implemented by* MITM *attacks.*

In this research, an MITM attack simulation was carried out using Ettercap with ARP Poisoning and Port Stealing attack techniques against an SDN topology created using the PPDIOO method. This scenario has the same effect of changing the victim's IP Address and MAC Address credentials in the ARP table. In addition, Port Stealing makes it possible to produce maximum impact to change the victim's switch communication on another switch. This results in the host being unable to communicate other than with the attacker. Collecting network latency data before and after the attack also proves that the two attack techniques do not affect the quality of network latency because there is no change in latency values with a value of 0.49s - 0.50s for packet delivery latency in network traffic.

Keywords: SDN, MITM, Ettercap, ARP Poisoning, Port Stealing, PPDIOO.