ABSTRACT

Software-Defined Networking (SDN) is a new development in the networking world that allows organization through programming. This concept is about the division of labor between network control and data management.One of the drawbacks of SDN implementation is the vulnerability to security attacks. This research focuses on this vulnerability and seeks to understand more deeply the mechanisms of two types of attacks known as Relay Attack and IP Spoofing.

This research implements Relay Attack and IP Spoofing attacks in the context of SDN and analyzes their impact on network quality, especially in terms of latency (delay) in data translation. Relay Attacks were tested using Scapy scripts, while IP Spoofing attacks were evaluated using Nmap with IP decoy and SYN Packet flooding techniques.

The analysis results include latency Quality of Service (QoS) assessment, Fake Link establishment that enables network traffic manipulation, and network latency index based on TIPHON standards. This research aims to uncover potential vulnerabilities in SDN and their impact on network security. In this context, the two attacks, namely Relay Attack and IP Spoofing, are also analyzed. During the attacks, Host 3 experienced "Not Good" delay with an average of 83,832.547 ms and 71,194.375 ms, while Host 5 experienced "Medium" delay with approximately 261.939 ms and 349.597 ms. Thus, Relay Attack generates Fake Links that can be utilized for manipulation, while IP Spoofing confuses the identity of the IP Host. The distance factor between the attacking and attacked hosts also plays an important role in determining the impact of an attack in a network.

Keywords: Relay Attack, IP Spoofing, Software Defined Network, Quality of Service, Network Vulnerability