ABSTRACT

5G is the latest generation of cellular technology to improve services from the previous generation and has many new features in the system. Along with the development of technology, there is an open source program that provides 5G core network services. The open source program allows developers, researchers or industries to form 5G networks themselves or can be said to be private cellular. But in the development of private cellular needs to consider the functional aspects and non-functional aspects.

In this final project, the author has succeeded in creating a 5G open source infrastructure platform, which will be filled with several attack simulation models or use cases that have been previously determined, after successfully determining the use case or attack simulation model. Then the author will analyze the open source infrastructure platform, to determine the effect or impact of each attack.

Therefore, based on the tests that have been carried out by the author, the author here has several use cases including, Randsource Attack DoS, Fuzzing, DNS Spoofing, and IDS Snort. From each use case or attack simulation, it has a different impact or impact, such as in Randsource Attack-DoS, the impact or impact can cause especially the services in the gNB to decrease, then for Fuzzing, the impact or impact on the 5G infrastructure platform is that connectivity on the infrastructure is disrupted, especially in the AMF signal protocol, then DNS Spoofing has an impact or impact, namely, causing tricking or diverting user interface pages to websites that have previously been designed or created, and IDS Snort has an impact or impact to detect attacks that have previously been carried out by Randsource Attack-DoS.

Keywords: Random Source Attack Denial of Service, Fuzzing, DNS Spoofing, IDS Snort, Open5gs, Core Network