

## **ABSTRACT**

*5G is the latest generation of cellular technology to improve services from the previous generation and provide many new capabilities in its system. Along with the development of technology, there are open source programs that provide 5G core network services. With the existence of an open source program, it allows developers, researchers, or industries to create their own 5G networks or it can be said to be private cellular. But in the development of mobile private it is necessary to consider its functional and non-functional aspects.*

*In this final project, the author simulates and tests the non-functional aspects, namely the security of the 5G core open source program. Testing was performed using denial of service (DoS) attack attempts. The attack technique uses flooding the server using TCP SYN signals and injecting packets for stress tests on the free5GC virtual network infrastructure. Thus, it can analyze the influence of attacks on the availability factor of network security.*

*Based on the test results, the network built when getting a DoS attack has an impact on network performance. The Free5GC server experienced a 68.83% increase in CPU resources during an attempted TCP SYN flood attack due to excessive load. Thus causing network performance parameters that refer to the quality of service (QoS) including throughput, packet loss, delay and jitter flowed by free5GC to decrease. Meanwhile, DoS attacks on components of the 5G network virtualization architecture have made the AMF Free5GC function stuck. Thus the user gets a denial of service from the core service.*

**Keywords:** *Denial of Service, free5GC, Mobile private*