ABSTRAK

5G merupakan teknologi seluler generasi terbaru untuk meningkatkan layanan dari generasi sebelumnya serta memberikan banyak kemampuan baru didalam sistemnya. Seiring perkembangan teknologi, terdapat program *open source* yang menyediakan layanan 5G *core network*. Dengan adanya program *open source* memungkinkan pengembang, peneliti, ataupun industry untuk membuat jaringan 5G sendiri atau bisa dikatakan privat seluler. Namun dalam pembangunan privat seluler perlu mempertimbangkan aspek fungsional dan non-fungsionalnya.

Pada tugas akhir ini, penulis melakukan simulasi dan pengujian terhadap aspek non-fungsional yakni keamanan program *open source 5G core*. Pengujian dilakukan dengan menggunakan percobaan serangan Denial of Service (DoS). Adapun teknik serangan menggunakan cara membanjiri server menggunakan sinyal TCP SYN dan menyuntikkan paket untuk *stres test* pada infrastruktur jaringan virtual *free5GC*. Dengan demikian dapat menganalisa pengaruh serangan terhadap faktor *availability* dari keamanan jaringan.

Berdasarkan hasil pengujian, jaringan yang dibangun ketika mendapatkan serangan DoS berdampak terhadap performansi jaringan. Server *Free5GC* mengalami peningkatan *resource* CPU 68.83 % saat percobaan serangan TCP SYN *flood* akibat beban yang berlebihan. Sehingga menyebabkan parameter network performance yang mengacu pada kualitas layanan atau Quality of services (QoS) meliputi throughput, paket loss, delay dan jitter yang dialirkan oleh *free5GC* menurun. Sedangkan serangan DoS pada komponen arsitektur virtualisasi jaringan 5G membuat fungsi AMF *Free5GC* macet. Dengan demikian pengguna mendapatkan penolakan layanan dari *core service*.

Kata Kunci: *Denial of Service*, *free5GC*, Privat seluler.