Evaluasi Jaringan Inti 5G Berbasis OpenAirInterface terhadap Serangan Denial of Service pada Fungsi Access and Mobility Management Function (AMF) dan User Plane Function (UPF) = Evaluation of 5G Core Network based on OpenAirInterface against Denial of Service Attacks on Access and Mobility Management Function (AMF) and User Plane Function (UPF)

Eriqo Arief Wicaksono, author

Abstrak

Denial of Service (DoS) merupakan jenis serangan keamanan yang menargetkan aspek ketersediaan layanan dengan cara menghabiskan sumber daya jaringan, sehingga pengguna tidak dapat mengakses layanan tersebut. Penelitian ini dilakukan untuk mengevaluasi ketahanan jaringan inti 5G berbasis OpenAirInterface (OAI) terhadap serangan DoS. Metodologi yang digunakan meliputi simulasi serangan packet replay terhadap Access and Mobility Management Function (AMF), dan serangan TCP SYN flood terhadap User Plane Function (UPF). Pengujian dilakukan menggunakan berbagai perangkat lunak seperti tcpreplay, 5greplay dan Hping3 dengan platform OAI yang dijalankan dalam lingkungan kontainerisasi sebagai target. Serangan replay menggunakan tcpreplay hanya menaikkan trafik AMF (Rx 5 MB/s, Tx 1 MB/s) dengan CPU usage kurang dari 5% secara rata-rata. Sebaliknya, serangan replay menggunakan 5greplay berhasil menaikkan CPU usage AMF hingga 144,28 %, yang menandakan pemanfaatan penuh lebih dari satu inti prosesor, sedangkan memori usage naik menjadi 35 MB, serangan ini memperpanjang durasi registrasi UE dari 15,44 s ke 37,86 s. Sementara itu, serangan TCP SYN flood terhadap UPF menggunakan Hping3 memberikan dampak yang cukup besar pula, ditandai dengan lonjakan penggunaan CPU hingga mencapai 106,3%, serta menyebabkan kenaikan packet loss hingga mencapai 73%. Hasil ini menegaskan pentingnya penerapan mekanisme mitigasi DoS yang kuat pada jaringan 5G.

.....Denial of Service (DoS) is a type of security attack that targets the availability aspect of a service by exhausting network resources, thereby preventing users from accessing the service. This study was conducted to evaluate the resilience of a 5G core network based on OpenAirInterface (OAI) against DoS attacks. The methodology involved simulating a packet replay attack targeting the Access and Mobility Management Function (AMF), as well as a TCP SYN flood attack targeting the User Plane Function (UPF). The tests were carried out using various tools such as tcpreplay, 5greplay, and Hping3, with the OAI platform deployed in a containerized environment as the target. The replay attack using tcpreplay only increased AMF traffic (Rx 5 MB/s, Tx 1 MB/s), with CPU usage remaining below 5% on average. In contrast, the replay attack using 5greplay increased AMF CPU usage up to 144.28%, indicating utilization of more than one processor core, while memory usage rose to 35 MB; this attack also extended the UE registration duration from 15.44 seconds to 37.86 seconds. Meanwhile, the TCP SYN flood attack on the UPF using Hping3 also had a significant impact, causing CPU usage to spike to 106.3% and packet loss to increase up to 73%. These findings highlight the critical need for strong DoS mitigation mechanisms in 5G networks.