Implementasi Dan Analisis Fuzzing 5G Replay Pada Jaringan 5G Prototype

1st Lukman Nul Hakim Abi
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fadhilahrafii@student.telkomuniversity.ac.id

2nd Rendy Munadi
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
rendymunadi@telkomuniversity.ac.id

3rd Fardan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fardanext@telkomuniversity.ac.id

***Abstrak* — Penelitian ini membahas pengujian keamanan infrastruktur jaringan 5G menggunakan metode Fuzzing dengan mereplay lalu lintas dari file pcap 5G menggunakan alat 5GReplay. Infrastruktur jaringan 5G diimplementasikan dengan memanfaatkan open-source komponen seperti Core Network Open5Gs dan UERANSIM. Metode Fuzzing digunakan untuk menguji potensi kerentanan dalam sistem core network terhadap serangan Fuzzing yang memanfaatkan celah dalam proses dekode pesan NGAP. Hasil pengujian menunjukkan bahwa core network mengalami kesalahan dalam dekode pesan NGAP saat terjadi serangan Fuzzing, yang mengindikasikan adanya potensi kerentanan dalam sistem. Pengujian ini menggarisbawahi perlunya perbaikan dalam sistem keamanan dan validasi pesan protokol yang lebih kuat untuk menjaga keamanan sistem jaringan 5G.**

***Kata kunci*— 5G, Fuzzing, 5GReplay, keamanan jaringan, Core Network Open5Gs, UERANSIM.**

I. PENDAHULUAN

Komunikasi seluler 5G lebih maju secara inovatif dibandingkan dengan seluler 4G komunikasi secara umum meliputi kecepatan, penggunaan protokol, dan konfigurasi jaringan. Jaringan 5G dikonfigurasi yang ditentukan oleh perangkat lunak dengan kecepatan 20 Gbps, 20 kali lebih cepat daripada evolusi sebelumnya (LTE), sementara jaringan inti 5G telah diubah dari tipe terpusat ke tipe desentralisasi untuk meminimalkan keterlambatan transmisi lalu lintas. Karena perubahan teknis tersebut, ITU-R menetapkan layanan 5G. Mengklasifikasikan layanan 5G menjadi broadband seluler yang ditingkatkan di mana kecepatan adalah elemen terpenting, kemudian bandwidth adalah elemen kunci, dan minimalisasi waktu latensi yang diperlukan.

II. KAJIAN TEORI

A. Fuzzing 5G Replay

fuzzing atau pengujian fuzz, adalah teknik pengujian perangkat lunak otomatis dengan cara menyuntikkan data yang salah, tidak terduga, atau acak ke dalam program komputer[1]. sedangkan 5G-Replay adalah program tools perangkat lunak berbasis open source untuk pengujian fuzz jaringan 5G. 5G replay memfasilitasi pengujian fungsional jaringan virtual 5G dengan memungkinkan paket jaringan diteruskan dari satu Network Interface Card (NIC) ke yang lain, dengan atau tanpa modifikasi[2]. Pengujian ini berfokus untuk mengubah lalu lintas 5G pada antarmuka N1 dan N2 antara RAN dan jaringan inti. Mekanisme yang digunakan adalah menyuntikkan paket yang sama atau dimodifikasi dengan paket yang sebelumnya ditangkap oleh Wireshark, skenario dari pengujian ini adalah mengevaluasi skalabilitas alat dengan cara membuat lalu lintas bandwidth tinggi menggunakan 5G-Replay untuk memutar ulang lalu lintas.

B. Core Network

Dalam arsitektur 5G yang baru berdasarkan SBA (Service Based Architecture) untuk setiap Network Function (NF) atau komponen fungsi virtual jaringan menyediakan layanan ke Network Functions (NFs) yang lain[3]. Pada infrastruktur jaringan 5G memiliki dua fase yaitu fase 5G Stand Alone (SA) dan 5G Non Stand Alone (NSA), sederhananya dalam 5G NSA masih menggunakan 4G core berbasis EPC (Evolved Packet Core) dan CUPS (Control and User Plane Separation). Tujuan utama dari sistem 5G untuk menyediakan konektivitas ke User Equipment (UE) melalui sistem registrasi, pengelolaan komunikasi antara komponen sistem 5G dengan bantuan protokol NAS (Non-Access Stratum) dan NGAP (NG Application Protocol). Komponen utama inti 5G dan protokol yang digunakan untuk komunikasi antara NF dan gNodeB antara lain adalah NRF, SCP, AMF, SMF, UPF, AUSF, UDM, UDR, PCF dan NSFF. Arsitektur ini mengatur bagaimana komunikasi dan aliran data diatur antara berbagai komponen dalam jaringan 5G, termasuk UE, NG-RAN, AMF, SMF, dan UPF. Semua ini adalah bagian integral dari 5G core SA (Stand Alone) Architecture, yang dirancang untuk mengoptimalkan kinerja jaringan 5G.

C. Ueransim

UERANSIM merupakan simulator open source untuk 5G UE dan 5G RAN (gNB). Sederhananya, UERANSIM dapat menggantikan ponsel 5G secara efektif Ini memiliki fungsi mekanis yang sama[4]. komunikasi yang dapat dikendalikan UERANSIM berisi antarmuka kontrol, yaitu komunikasi antara RAN dan AMF. Antarmuka pengguna, yaitu komunikasi antara RAN dan UPF, yaitu antarmuka radio Komunikasi antara UE dan RAN.

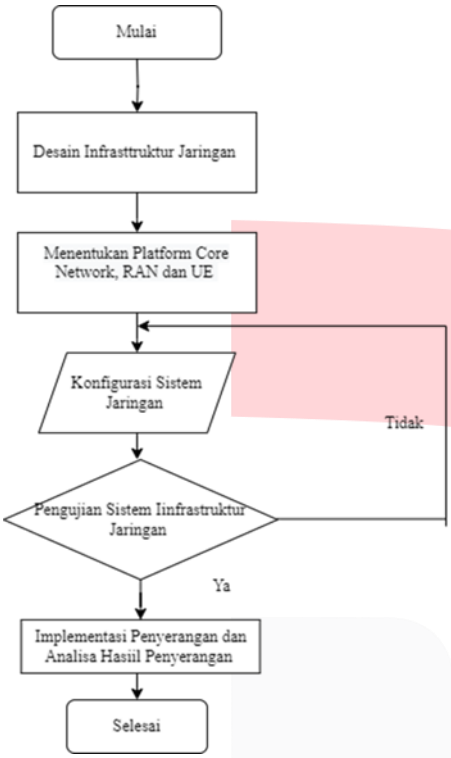
III. METODE

Metode penelitian pada tugas akhir ini dimulai dari melakukan desain system, desain simulasi yang akan

digunakan sebagai jaringan prototype 5G, kemudian perangkat keras dengan minimum spesifikasi yang akan digunakan, dan pernagkat lunak yang digunakan.

A. Desain Sistem

Sebelum melakukan simulasi, dilakukan terlebih dahulu desain untuk system yang akan digunakan nantinya



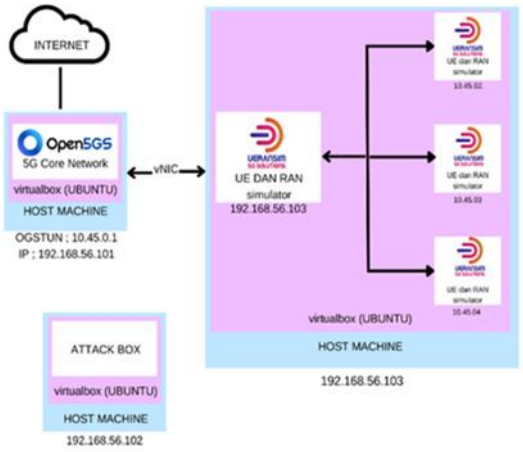
GAMBAR 3.1
Flowchart Rencana Desain Sistem

Seperti pada gambar diatas, terdapat flowchart atau alur kerja sebelum dilakukan implementasi system yang sesungguhnya. Dapat dijelaskan pada flowchart yaitu,

1. Mendesain infrastruktur jaringan
2. Menentukan platform apa yang akan dipakai untuk Core Network, Ran dan UE
3. Mengkonfigurasi sistem
4. Pengujian sistem yang sudah dikonfigurasi, jika sudah berjalan dengan baik masuk ke tahap selanjutnya. Tetapi, jika masih terjadi kesalahan maka kembali ke tahap konfigurasi sistem
5. Jika sistem Infrastruktur sudah berjalan masuk ke tahap implementasi penyerangan di sistem infrastruktur untuk mengambil data hasil penyerangannya dan dilakukan analisa terhadap penyerangan yang sudah diimplementasikan
6. Selesai.

B. Desain Simulasi

Gambar dibawah merupakan model dari system yang akan dilakukan untuk pengujian penyerangan

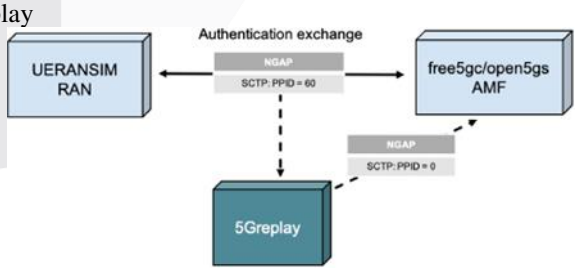


GAMBAR 3.2
Skema Infrastruktur 5G

Penulis akan membangun perangkat yang akan menyediakan end-to-end 5G infrastruktur yang memiliki komponen Core Network, RAN, dan UE. Platform infrastruktur yang sudah berhasil dirancang akan digunakan untuk melakukan pemodelan serangan yang mana pada tahap ini penulis akan menganalisis dan mendapatkan informasi mengenai model dan cara kerja serangan termasuk untuk memvalidasi serangan tersebut serta mengetahui dampak dan mendeteksi keamanan pada infrastruktur teknologi jaringan 5G.

C. Attack Infrastructure 5G Replay

Fuzzing, sebagai metode pengujian perangkat lunak yang mengirimkan input yang tidak valid atau acak ke sistem, serangan fuzzing 5G replay muncul sebagai ancaman yang memanfaatkan ulang data dan respons sebelumnya untuk mengganggu integritas, keamanan, dan ketersediaan jaringan yang penting. Mekanisme yang digunakan adalah menyuntikkan paket yang sama atau dimodifikasi dengan paket yang sebelumnya ditangkap oleh Wireshark, skenario dari pengujian ini adalah mengevaluasi skalabilitas alat dengan cara membuat lalu lintas bandwidth tinggi menggunakan 5G-Replay untuk memutar ulang lalu lintas yang di rekam atau di simpan dalam file pcap. Pada gambar dibawah ini menampilkan skenario fuzzing 5G replay



GAMBAR 3.3
Skema Pengiriman Paket NGAP yang Cacat

Dengan membuat beberapa salinan dan mengirimkannya ke open5gs. Tujuannya untuk mengacaukan layanan kritis yang bergantung pada 5G dan mengganggu konektivitas perangkat. Penulis akan mengamati komponen yang berdampak, terutama pada komponen AMF dari core network open5gs yang akan mengalami kerusakan. Skenario kasus ini mengevaluasi kemampuan 5G-Replay untuk membuat dan mengirim secara sistematis paket yang salah

bentuk, ke jaringan core 5G, untuk mengevaluasi ketahanannya terhadap entri tak terduga saat run-time berikut adalah perintah untuk melakukan Fuzzing 5G-Replay.

```
sudo ./5greplay replay -t 5g-sa.pcap -Xforward.nb-copies=2000 -Xforward.default=FORWARD > log.txt 2>&1
```

Untuk perintah yang dijalankan memiliki opsi yang diberikan termasuk menggandakan salinan paket sebanyak 2000 kali dan mengatur pengaturan default untuk penerusan paket. Output hasil dan pesan kesalahan akan diarahkan ke file "log.txt" untuk referensi atau analisis lebih lanjut.

IV. HASIL DAN PEMBAHASAN

A. Pengujian Fungsionalitas Sistem

Pengujian fungsionalitas dilakukan untuk memastikanCore Network Open5Gs dan UERANSIM bekerja dan bisa berkomunikasi dengan baik. Pengujian dikatakan berhasil jika GNB dan UE UERANSIM bisa terhubung kepada Core Network Open5Gs. Dan beberapa komponen Core Network Open5Gs berfungsi seperti yang diharapkan. Simulasi Infrastruktur kami dijalankan oleh 2 buah virtual mesin, dan masing-masing viirtual mesin menggunakan sistem operasi ubuntu versi 22.04. Selain itu, dilakukan test atau pengujian komponen status open5gs-AMFD yang berjalan baik, seperti pada gambar dibawah.

GAMBAR 4.1
Status Open 5Gs AMFD

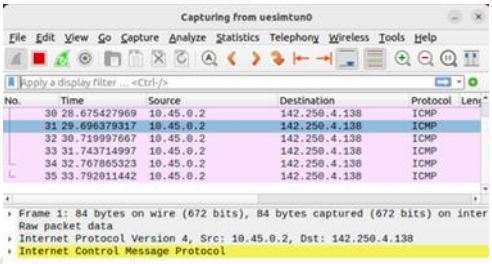
Pada gambar diatas dapat terlihat bahwa, komponen tersebut dapat berjalan dengan baik. Kemudian, dilakukan konfigurasi antara gNB dengan core network, seperti yang tertera pada gambar dibawah.

GAMBAR 4.2
Status gNB Terhubung ke Core Network

komponen GNB telah berhasil terhubung dengan komponen inti jaringan. Setelah GNB melakukan prosedur NG Setup yang berhasil dan terhubung melalui SCTP. Dengan berhasil nya penghubungan antara komponen GNB dan komponen inti jaringan, system siap untuk melakukan registrasi dan penghubungan komponen UE kepada komponen GNB dan juga komponen inti jaringan. Kemudian dapat ditandai pada gambar dibawah, bahwa status dari UE (*User Equipment*) dengan gNB berhasil terhubung

GAMBAR 4.3
Staus UE Terhubung Dengan gNB

Dengan berhasilnya proses penghubungan UE yang ditunjukan pada gambar diatas, komponen gNB dan Inti Jaringan, semua tahapan yang diperlukan dalam membangun Jaringan 5G sederhana telah berhasil di implementasikan. Proses ini dimulai dengan UE yang melakukan pemindaian terhadap Sel GNB yang sesuai dan melakukan prosedur registrasi pada komponen Inti Jaringan Open5GS. Setelah UE berhasil terhubung dengan GNB, proses RRC setup, autentikasi, dan pembentukan PDU session juga berhasil dilakukan. Serta telah memasuki status MM-REGISTERED/NORMAL -SERVICE yang mengindikasikan bahwa UE siap untuk mengakses berbagai layanan Jaringan 5G. Kemdian untuk memastikan dilakukan test ping pada google dan percobaan tersebut berhasil. Dengan yang tertera pada gambar dibawah



GAMBAR 4.4
Ping Google

Pada gambar diatas menunjukan bahwa konektivitasnya telah siap untuk mengakses internet.

B. Pengujian Fuzzing 5G Replay

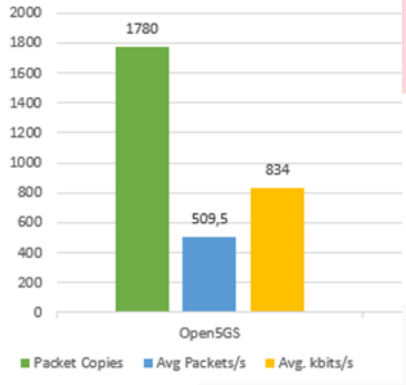
Setelah mengimplementasikan infrastruktur 5G yang selesai, kami melakukan pengujian penetrasi dengan menggunakan metode Fuzzing dengan mereplay lalu lintas dari file pcap 5G menggunakan tools 5GReplay. Serangan Fuzzing ini diarahkan ke virtual machine yang menjalankan open5gs sebagai core network 5G. Selama pengujian, kami mengamati log yang dihasilkan oleh core network saat terjadi Fuzzing.

Dalam log yang dihasilkan oleh open5gs saat terjadi Fuzzing, terdapat beberapa peringatan dan kesalahan yang muncul. Log menunjukkan bahwa terjadi kesalahan dalam dekode pesan NGAP yang diterima oleh core network. Beberapa peringatan mengenai gagal dekode ASN-PDU dan NGAP-PDU juga terlihat. Kesalahan dekode ini mengindikasikan adanya masalah dalam menguraikan pesan

protokol NGAP yang berasal dari file pcap yang direplay dilihat dari gambar 4.5.

GAMBAR 4.5
Status Open5Gs Ketika Dilakukan Fuzzing

Selama dilakukan Fuzzing terhadap core network, pada gambar 4.5 log menunjukkan bahwa terjadi serangkaian kesalahan dalam dekode pesan NGAP yang masuk ke core network. Gagalnya dekode ASN-PDU dan NGAP-PDU mengindikasikan bahwa protokol NGAP yang diterima oleh core network memiliki format yang tidak valid atau tidak sesuai dengan harapan. Hal ini dapat menunjukkan bahwa serangan Fuzzing ini berhasil memanfaatkan kerentanan dalam proses dekode pesan pada core network.



GAMBAR 4.6
Ketahanan Layanan AMF Terhadap Traffic Replaying

Dalam data chart pada gambar 4.6, terlihat bahwa selama pengujian Fuzzing, terdapat total 1780 salinan paket yang berhasil direplay. Rata-rata laju paket adalah 509,5 paket per detik, dengan rata-rata laju transfer data sekitar 834 kbit per detik.

V. KESIMPULAN

Dari hasil pengujian metode Fuzzing dengan mereplay lalu lintas dari file pcap 5G menggunakan tools 5GReplay, ditemukan bahwa core network mengalami kesalahan dalam dekode pesan NGAP saat terjadi Fuzzing. Hal ini mengindikasikan bahwa sistem core network rentan terhadap serangan Fuzzing yang dapat memanfaatkan celah dalam proses dekode pesan. Oleh karena itu, pengujian Fuzzing ini telah membuktikan adanya potensi kerentanan dalam sistem core network dan menyoroti perlunya perbaikan dalam sistem keamanan dan validasi pesan protokol yang lebih kuat. Langkah-langkah pengamanan tambahan harus diambil untuk mengatasi masalah ini dan menjaga keamanan sistem secara keseluruhan

REFERENSI

[1] wikipedia.org, (last edited 2023,7 agustus). Fuzzing. Diakses pada 2 Agustus 2023, dari https://en.wikipedia.org/wiki/Fuzzing.

[2] Salazar dkk, (2021) “5Greplay: a 5G Network Traffic Fuzzer - Application to Attack Injection,” ARES 2021, August 17–20, 2021, Vienna, Austria arXiv:2304.05719v1 [cs.NI] page 12.

[3] Aladren, Domingo., Carmen, Del Maria. (2022). A Degree Thesis: Log-based monitoring, detection and automated correction of anomalies in the 5G core.

[4] github.com. (2022, 13 Januari). Aligungr/UERANSIM. Diakses pada 22 Juli 2023, dari https://github.com/aligungr/UERANSIM.