# Implementasi Dan Analisis IDS Snort Pada Jaringan 5G Prototype

1st Ismail Choiri
*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* — Jurnal ini membahas tentang keamanan dan penetrasi jaringan seluler 5G melalui pengujian fungsionalitas, simulasi serangan Denial of Service (DoS), dan implementasi sistem Intrusion Detection System (IDS) menggunakan Snort. Keamanan dalam jaringan nirkabel semakin krusial seiring perkembangan generasi jaringan seluler. Dengan fokus pada 5G, penulis menjelaskan desain sistem, termasuk komponen Core Network, RAN, dan UE, serta mengimplementasikan teknologi UERANSIM dan IDS Snort. Pengujian fungsionalitas mengkonfirmasi konektivitas antara komponen dan layanan 5G. Simulasi serangan DoS dilakukan dengan metode flood randsource, sementara IDS Snort dijalankan untuk mendeteksi dan melacak serangan tersebut. Hasil pengujian menunjukkan pentingnya pendeteksian dini serangan dan respons yang cepat dalam memitigasi ancaman keamanan.**

***Kata kunci*— 5G, Denial of Service (DoS), Intrusion Detection System (IDS), Snort.**

## I. PENDAHULUAN

Sistem komunikasi nirkabel telah rentan terhadap kerentanan keamanan sejak awal. Di jaringan nirkabel generasi pertama (1G), ponsel dan saluran nirkabel ditargetkan untuk kloning ilegal dan menyamar. Pada generasi kedua (2G) nirkabel jaringan, spam pesan menjadi umum tidak hanya untuk serangan meluas tetapi menyuntikkan informasi palsu atau menyiarkan informasi pemasaran yang tidak diinginkan. Pada generasi ketiga (3G) jaringan nirkabel, komunikasi berbasis IP memungkinkan migrasi kerentanan dan tantangan keamanan Internet di domain nirkabel. Dengan meningkatnya kebutuhan berbasis IP komunikasi, jaringan seluler Generasi keempat (4G). memungkinkan proliferasi perangkat pintar, lalu lintas multimedia, dan layanan baru ke dalam domain seluler Langkah penting dalam memfasilitasi jaringan yang sehat adalah memantau dan menganalisis lalu lintas persinyalan ketika melintasi perbatasan jaringan, yang memungkinkan untuk menangkap kesalahan konfigurasi dan suguhan potensial.

## II. KAJIAN TEORI

### A. 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[1]. 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.

### B. 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[2]. 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.

### C. IDS Snort

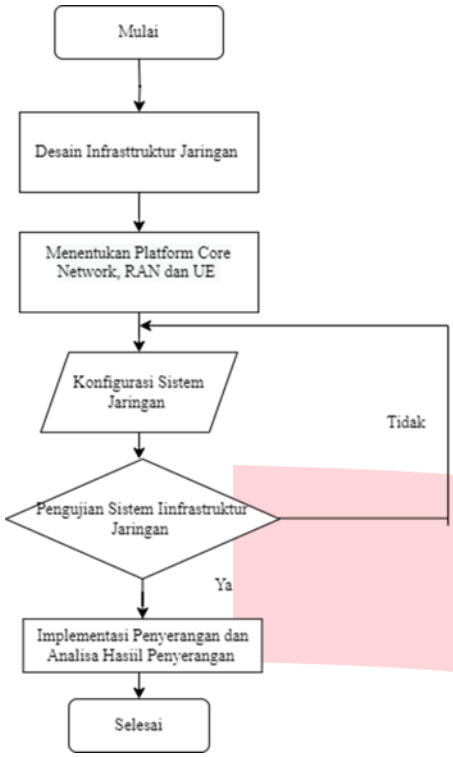
Dalam sistem Intrusion Detection System (IDS) membantu mendeteksi aktivitas mencurigakan pada sistem atau jaringan[3]. Salah satu alat yang dapat digunakan adalah snort. Snort adalah perangkat lunak yang mendeteksi penyusup dan dapat menganalisa paket yang melewati jaringan secara real time Intrusion Detection System (IDS) diterapkan karena mampu mendeteksi paket-paket berbahaya pada jaringan, bekerja sebagai pendeteksi aktivitas yang mencurigakan pada jaringan.

## 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.



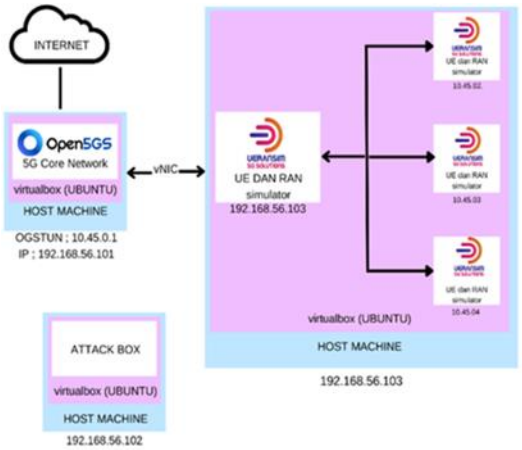

GAMBAR 3.1
Flowchart Rencana Desain Sistem

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

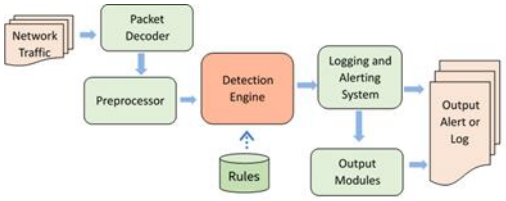



GAMBAR 3.2
Skema Infrastruktur 5G

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. IDS Snort

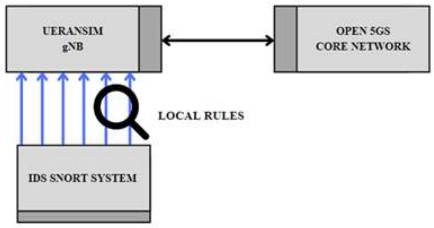
Snort beroperasi sebagai sistem deteksi penyusupan sumber terbuka yang kuat. Sistem ini memonitor lalu lintas jaringan,menganalisis isi paket untuk pola yang mencurigakan berdasarkan aturan yang telah ditentukan, dan mendeteksi anomali atau serangan. Ketika kecocokan ditemukan, Snort mengambil tindakan yang telah dikonfigurasi seperti pemberitahuan atau pencatatan. Sangat efisien, dapat dikustomisasi, dan merupakan alat yang sangat penting untuk meningkatkan keamanan jaringan. Pada penelitian ini dilakukan serangan DoS jenis Randsource, untuk melihat sejauh mana pengukuran kinerja keamanan data dari simulasi serangan pada jaringan infrastruktur 5G Sistem Snort diinisialisasi dan dijalankan dalam mode Intrusion Detection System (IDS). Snort menginisialisasi output preprocessor, dan plug-in berikut skema dari sistem Intrusion Detection System (IDS).




GAMBAR 3.3
Skema sistem IDS

Pada gambar 3.3 diatas dapat dilihat Intrusion Detection System (IDS) diimplementasikan karena dapat mendeteksi paket berbahaya di jaringan, bekerja sebagai pendeteksi

aktivitas mencurigakan di jaringan [4]. Sistem Intrusion Detection System (IDS) digunakan karena keamanan jaringan belum efektif/kompeten untuk menjaga jaringan. Menambahkan keadaan internal atau sistem pencegahan intrusi adalah salah satu cara untuk mendeteksi dan mencegah serangan [5]. Untuk pendeteksian snort akan dilakukan pada gNB yang diserang oleh DoS, pada gambar3.4 dibawah memperlihatkan skema dari pendeteksian sistem IDS Snort.




GAMBAR 3.4
Skenario IDS Snort

## IV. HASIL DAN PEMBAHASAN

### A. Pengujian Fungsionalitas Sistem

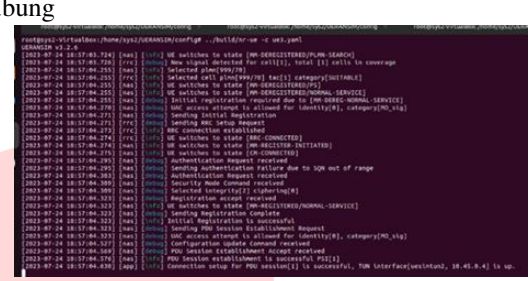
Pengujian fungsionalitas dilakukan untuk memastikanCore Network Open5Gs dan UERANSIM bekerja dan bisa berkomunikasi dengan baik. Pengujian dikatakan berhasil jika GNB dan UE UERANSIM bisa terhubung kepada Core Network Open5Gs. Dan beberapa komponen Core Network Open5Gs berfungsi seperti yang diharapkan. 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

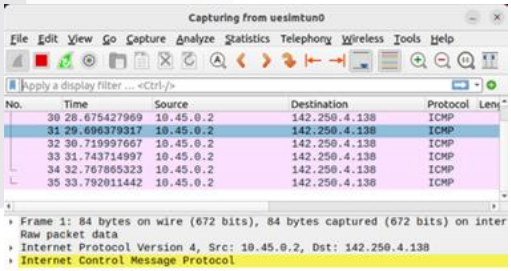
GAMBAR 4.2
Status gNB Terhubung ke Core Network

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



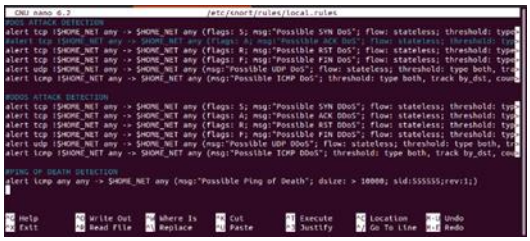

GAMBAR 4.4
Ping Google

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

### B. Pengujian IDS Snort

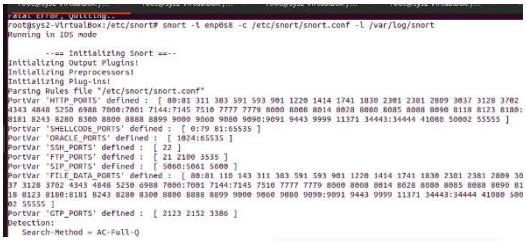
Dalam rangka menguji penetrasi infrastruktur 5G yang telah selesai dikonfigurasi, kami melakukan serangan Denial of Service (DoS) dengan menggunakan metode DoS flood randsource menggunakan perangkat hping3. Serangan ini ditargetkan ke virtual machine yang berisi simulasi

UERANSIM gNB dan UE. Selanjutnya, untuk menjaga keamanan dan deteksi serangan, kami mengimplementasikan sistem Intrusion Detection System (IDS) menggunakan Snort versi 2.9.15.1 dengan aturan lokal yang telah disusun pada gambar 4.5



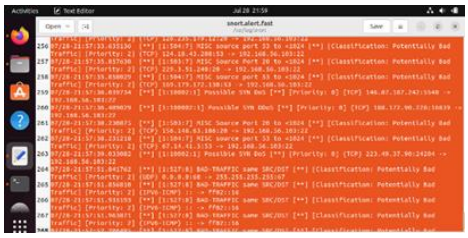
GAMBAR 4.5
Lokal Rules Snort

Pada gambar 4.5, aturan lokal yang diterapkan pada Snort, terdapat beberapa deteksi yang dilakukan terhadap jenis-jenis serangan tertentu. Aturan tersebut secara spesifik mendeteksi serangan Denial of Service (DoS) dan Distributed Denial of Service (DDoS) yang menggunakan berbagai tipe paket seperti SYN, ACK, RST, FIN, UDP, dan ICMP. Selain itu, juga terdapat deteksi serangan "Ping of Death" yang mendeteksi paket ICMP yang memiliki ukuran lebih dari 10000 byte. Aturan-aturan ini bertujuan untuk memberikan tanda-tanda dini ketika terjadi serangan terhadap infrastruktur.



GAMBAR 4.6
Snort Dijalankan

Pada gambar 4.6 menampilkan Ketika menjalankan Snort dengan perintah "snort -i enp0s8 -c /etc/snort/snort.conf -1 /var/log/snort", sistem Snort diinisialisasi dan berjalan dalam mode Intrusion Detection System (IDS). Snort melakukan inisialisasi output plugins, preprocessors, dan plug-ins yang diperlukan. Aturan-aturan dari berkas konfigurasi "/etc/snort/snort.conf" kemudian dianalisis untuk mendeteksi potensi serangan. Snort akan melacak dan menganalisis lalu lintas jaringan yang melewati antarmuka "enp0s8" dan mencatat hasil deteksi dalam berkas log yang ditentukan, yaitu "/var/log/snort"



GAMBAR 4.7
Tampilan Peringatan pada IDS Snort

Dalam berkas log "alert" yang dihasilkan di gambar 4.7 diatas, terdapat informasi mengenai deteksi serangan yang terjadi. Setiap baris log menyertakan informasi seperti alamat IP sumber dan tujuan, port, protokol, pesan deteksi, dan waktu deteksi. Beberapa contoh log menunjukkan deteksi serangan potensial seperti serangan SYN DoS, SYN DDoS, dan "Ping of Death". Pesan deteksi ini memberikan indikasi jenis serangan yang terjadi dan parameter yang digunakan dalam deteksi

## V. KESIMPULAN

Jika sistem IDS Snort mendeteksi serangan Denial of Service (DoS) yang menggunakan metode DoS flood randsource, langkah pertama yang harus dilakukan adalah melakukan identifikasi dan konfirmasi serangan yang terjadi. Setelah serangan dikonfirmasi, tindakan selanjutnya adalah melakukan mitigasi serangan dengan mengisolasi sumber serangan, memblokir alamat IP yang terlibat, atau mengalihkan lalu lintas serangan ke sistem penyaringan. Selanjutnya, dilakukan analisis mendalam terhadap serangan untuk memahami karakteristik dan sumber serangan, guna meningkatkan sistem pertahanan kedepannya. Seluruh tindakan yang diambil harus sesuai dengan kebijakan keamanan yang telah ditentukan sebelumnya.

## REFERENSI

[1] International Telecommunication Union Radiocommunication. Detailed Specifications of the Terrestrial Radio Interfaces of International Mobile Telecommunications-2020 (2020)

[2] Damayanti dkk. (2022). Desain and Build 4G Open Radio Access Network at SmartLab Politeknik Negeri Jakarta. Doi: 10.31289/jite.v6i2.7537

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

[4] Open5gs.org. (2022, 18 Juni). https://open5gs.org/. Diakses pada 22 Juli 2023, dari https://open5gs.org/open5gs/docs/tutorial/01-your-first-lte/

[5] Pande, S., Khamparia, A., Gupta, D., and Thanh, D.N. DDOS Detection using Machine Learning Technique. In Recent Studies on Computational Intelligence, pp. 59-68, 2021.