

DAFTAR GAMBAR

Gambar 1.1 Mengenai Ancaman pada 5G[5]	2
Gambar 3.1 Sistem Core Network dan gNB dalam satu VM.....	13
Gambar 3.2 Flowchart Rencana Desain Sistem	17
Gambar 3.3 Jadwal Pengerjaan.....	18
Gambar 4.1 Infrastruktur 5G SA [10].....	21
Gambar 4.2 Arsitektur Open5Gs [11]	22
Gambar 4.3 Status Pelayanan Open5GS-AMFD.....	23
Gambar 4.4 Status gNB Berjalan.....	23
Gambar 4.5 UE Berhasil Terhubung	24
Gambar 4.6 File PCAP Wireshark Lalu Lintas Jaringan.....	25
Gambar 4.7 Skema Penyerangan RANDBSOURCE-DoS	26
Gambar 4.8 Skema pengiriman paket NGAP yang cacat [15]	27
Gambar 4.9 Skema Penyerangan DNS Spoofing	28
Gambar 4.10 File PCAP Wireshark Hping3.....	29
Gambar 4.11 Skema Intrusion Prevention system [20]	32
Gambar 5.1 Skema Infrastruktur 5G	37
Gambar 5.2 Status Open5gs-AMFD.....	38
Gambar 5.3 Status gNB Terhubung ke Core Network.....	38
Gambar 5.4 Status UE Terhubung Dengan gNB.....	39
Gambar 5.5 Ping Google	39
Gambar 5.6 Kondisi Normal Open5gs	40
Gambar 5.7 Kondisi CPU Usage Sebelum dan Sesudah Penyerangan	41
Gambar 5.8 Kondisi Memory Usage Sebelum dan Sesudah Penyerangan	41
Gambar 5.9 Kondisi Throughput Sebelum dan Sesudah Penyerangan	42
Gambar 5.10 Kondisi Packet Loss Sebelum dan Sesudah Penyerangan.....	43
Gambar 5.11 Kondisi Delay Sebelum dan Sesudah Penyerangan	43
Gambar 5.12 Jitter Sebelum dan Sesudah Penyerangan.....	44
Gambar 5.13 Local Rules Snort.....	45
Gambar 5.14 Snort Dijalankan	46
Gambar 5.15 Tampilan Peringatan Pada IDS Snort	46
Gambar 5.16 Status Open 5Gs ketika dilakukan Fuzzing	48
Gambar 5.17 Ketahanan Layanan AMF Terhadap Traffic Replaying	48

Gambar 5.18 Status Penyerangan	50
Gambar 5.19 Alamat IP Penyerang	50
Gambar 5.20 Aktivasi Apache2.....	51
Gambar 5.21 Directory Serangan	51
Gambar 5.22 DNS Config Pada Ettercap	52
Gambar 5.23 Aktifasi Serangan Spoofing	53
Gambar 5.24 Host Scanning	53
Gambar 5.25 Aktifasi DNS Spoofing.....	54
Gambar 5.26 Status Web Terspoofing.....	55
Gambar 5.27 Web Open5gs Sebelum Serangan.....	56
Gambar 5.28 Kondisi Web Open5gs Setelah Serangan	56