

DAFTAR GAMBAR

Gambar 1.1. Logo Snort.....	10
Gambar 1.2. Logo Suricata	11
Gambar 1.3. Logo Zeek	12
Gambar 3.1. Diagram Blok.....	55
Gambar 3.2. Flowchart Sistem.....	56
Gambar 3.3. Flowchart IDS	58
Gambar 3.4. Flowchart Sistem Notifikasi.....	59
Gambar 3.5. Use Case Diagram.....	61
Gambar 3.6. DFD Level 0.....	62
Gambar 3.7. DFD Level 1.....	63
Gambar 3.8. DFD Level 2.....	64
Gambar 3.9. Threat Modeling STRIDE.....	70
Gambar 4.1. Komponen perakitan Raspberry Pi 5	80
Gambar 4.2. Nyala LED indikator daya aktif.....	81
Gambar 4.3. Hasil akhir perakitan Raspberry Pi 5 1	82
Gambar 4.4. Hasil akhir perakitan Raspberry Pi 5 2	82
Gambar 4.5. Hasil Pemasangan SD Card pada Raspberry Pi 5	83
Gambar 4.6. Tampilan saat program Snort berjalan	107
Gambar 4.7. Tampilan program notifikasi alert telegram.....	108
Gambar 4.8. Group Notifikasi alert telegram	108
Gambar 4.9. Tampilan Notifikasi yang dikirim ke telegram	109
Gambar 4.10. Tampilan Alert intrusi yang dicatat di alert.fast.txt	109
Gambar 4.11. Tampilan commit/push arsip log ke repository GitHub.....	110
Gambar 4.12. Tampilan Repository GitHub.....	111
Gambar 5.1. Grafik beban dan waktu pengujian Stress Test CPU	119
Gambar 5.2. Grafik Hasil Suhu pengujian Stress Test CPU.....	119
Gambar 5.3. Grafik load yang digunakan pada pengujian Memori.....	120
Gambar 5.4. Grafik Pemakaian Memori pada pengujian Memori.....	120

Gambar 5.5. Grafik Suhu saat Pengujian Memori	121
Gambar 5.6. Grafik Suhu saat Pengujian Memori	121
Gambar 5.7. Hasil Pengujian Kecepatan SD Card	122
Gambar 5.8. Perbandingan Kecepatan antara dd dan fio	122
Gambar 5.9. Hasil keseluruhan kecepatan dalam pengujian storage	123
Gambar 5.10. Perbandingan Download dan Upload Wi-Fi	123
Gambar 5.11. Hasil bitrate/stream Upload	124
Gambar 5.12. Hasil bitrate/stream Download	124
Gambar 5.13. Perbandingan Download dan Upload Ethernet	124
Gambar 5.14. Hasil bitrate/stream Download Ethernet	125
Gambar 5.15. Hasil bitrate/stream Upload Ethernet	125
Gambar 5.16. Perbandingan Download dan Upload Bridge	125
Gambar 5.17. Hasil bitrate/stream Download Bridge	126
Gambar 5.18. Hasil bitrate/stream Upload Bridge	126
Gambar 5.19. Daftar library penting sudah terpasang pada Snort	127
Gambar 5.20. Snort.conf sudah berjalan tanpa ada error	127
Gambar 5.21. Pengujian Penggunaan snort yang sudah tanpa kendala	128
Gambar 5.22. Pengujian Serangan DoS pada IDS	128
Gambar 5.23. Pengujian Serangan DNS Spoofing dan BruteForce pada IDS	129
Gambar 5.24. Pengujian Serangan Reconnaissance pada IDS	129
Gambar 5.25. Pengujian Serangan berbasis Web pada IDS	130
Gambar 5.26. Pengujian Serangan Mirai Botnet pada IDS	130
Gambar 5.27. Hasil Pengujian False Positive Rate Rules IDS	131
Gambar 5.28. Hasil Pengujian False Positive Rate Setelah Perbaikan	131
Gambar 5.29. Hasil Pengujian Rule Drop Mode IPS	132
Gambar 5.30. Hasil Pengujian Rule Reject Mode IPS	133
Gambar 5.31. Ringkasan Statistik Utama Pengujian Latensi	134
Gambar 5.32. Grafik Tingkat Keberhasilan Notifikasi Berdasarkan Waktu	135
Gambar 5.33. Grafik Tren Latensi per Batch	136

Gambar 5.34. Ringkasan Statistik Utama Pengujian Rate Limit.....	137
Gambar 5.35. Grafik Distribusi Status Notifikasi.....	137
Gambar 5.36. Grafik Penggunaan CPU Selama Stress Test.....	138
Gambar 5.37. Grafik Penggunaan Memori Selama Stress Test.....	139
Gambar 5.38. Grafik Suhu Perangkat Selama Stress Test.....	139
Gambar 5.39. Grafik Tingkat Keberhasilan Rotasi dan Unggah Log.....	140
Gambar 5.40. Grafik Waktu Eksekusi Proses Rotasi dan Unggah Log.....	141