

DAFTAR GAMBAR

Gambar 3. 1 Blok Arsitektur Sistem Pencegahan Serangan Siber	23
Gambar 3. 2 Diagram Alir Sistem Serangan Siber.....	25
Gambar 4. 1 Topologi Implementasi.....	32
Gambar 4. 2 Langkah - Langkah Implementasi Sistem Solusi	34
Gambar 4.3 Verifikasi instalasi Snort 3.....	35
Gambar 4. 4 Verifikasi hasil instalasi plugin DPX.....	37
Gambar 4. 5 Diagram Alir perancangan model Machine Learning	38
Gambar 4. 6 Tampilan Dashboard di API	42
Gambar 4. 7 Tampilan Wazuh Dashboard	43
Gambar 4. 8. Proses deployment agent pada Wazuh Dashboard	44
Gambar 4. 9 Verifikasi hasil dari instalasi Wazuh Agent dari Wazuh Dashboard.....	45
Gambar 4. 10 Konfigurasi logging pada Wazuh Agent	46
Gambar 4. 11 Konfigurasi ruleset untuk logging pada Wazuh Server	47
Gambar 5. 1 Konfigurasi Network pada VM Snort.....	51
Gambar 5. 2 Log Serangan Brute Force (R2L)	54
Gambar 5. 3 Log Serangan Exploit (U2R).....	55
Gambar 5. 4 Log Serangan SYN Flood.....	55
Gambar 5. 5 Log Serangan UDP Flood.....	56
Gambar 5. 6 Log Serangan Full Port Scan	56
Gambar 5. 7 Log Serangan IP Sweep.....	57
Gambar 5. 8 Classification Report Naive Baayes	58
Gambar 5. 9 Classification Report XGBoost	59
Gambar 5. 10 Classification Report Neural Network.....	60
Gambar 5. 11 Classification Report K-Means.....	61
Gambar 5. 12 Pengujian Trafik Normal	62
Gambar 5. 13 Grafik Hasil Pengujian Trafik Normal	63
Gambar 5. 14 Pengujian Serangan IP Sweep	64
Gambar 5. 15 Grafik Hasil Pengujian IP Sweep antar Model ML	65
Gambar 5. 16 Grafik Perbandingan Deteksi IP Sweep Rule Based dan ML	66
Gambar 5. 17 Pengujian Serangan Full Port Scan.....	67
Gambar 5. 18 Grafik Hasil Pengujian Full Port Scan.....	68
Gambar 5. 19 Grafik Perbandingan Deteksi Full Port Scan Rule Based dan ML.....	69

Gambar 5. 20 Pengujian Serangan SYN Flood	70
Gambar 5. 21 Grafik Hasil Pengujian SYN Flood	70
Gambar 5. 22 Grafik Perbandingan Deteksi SYN Flood Rule Based dan ML	71
Gambar 5. 23 Pengujian Serangan UDP Flood	72
Gambar 5. 24 Grafik Hasil Pengujian UDP Flood	73
Gambar 5. 25 Grafik Perbandingan Deteksi UDP Flood Rule Based dan ML	74
Gambar 5. 26 Pengujian Serangan FTP Brute Force.....	75
Gambar 5. 27 Grafik Hasil Pengujian R2L Brute Force	75
Gambar 5. 28 Perbandingan Deteksi FTP Brute Force Rule Based dan ML	76
Gambar 5. 29 Pengujian Serangan U2R Exploit	77
Gambar 5. 30 Grafik Hasil Pengujian U2R Exploit	78
Gambar 5. 31 Perbandingan Deteksi U2R Exploit Rule Based dan ML	79
Gambar 5. 32 Hasil Alert Wazuh SIEM.....	80