DAFTAR ISI

LEMBAR PERSEMBAHAN **2**
LEMBAR PENGESAHAN ..... **i**
LEMBAR PENGESAHAN PEMBIMBING LAPANGAN MAGANG ..... **ii**
KATA PENGANTAR ..... **iii**
PERNYATAAN ..... **iv**
DAFTAR ISI ..... **v**
DAFTAR GAMBAR ..... **viii**
DAFTAR TABEL ..... **x**
BAB I PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah dan Solusi 2
1.3 Tujuan 2
1.4 Batasan Masalah 2
1.5 Penjadwalan Kerja 2
BAB II STUDI PUSTAKA **4**
2.1 Wazuh 4
2.1.1 Fungsi Wazuh 4
2.1.2 Arsitektur Wazuh 5
2.1.3 Cara Kerja Wazuh 7
2.1.4 Spesifikasi Minimal 8
2.1.5 Port Yang Dibutuhkan Wazuh 8
2.2 Intrusion Detection System 9
2.2.1 Fungsi Intrusion Detection System 9
2.2.2 Jenis-Jenis Intrusion Detection System 9
2.2.3 Komponen Intrusion Detection System 10
2.2.4 Metode Deteksi Intrusion Detection System 10
2.3 Gambaran Umum Institusi 10
2.3.1 Struktur Organisasi institusi 12
2.4 Divisi Kerja 13

BAB III ANALISIS PEKERJAAN 15
3.1 Deskripsi dan Alur Pekerjaan 15
3.2 Analisis Sistem 16
3.2.1 Gambaran Sistem Saat Ini 16
3.2.2 Pengembangan Sistem 17
3.3 Kebutuhan Perangkat Kerja 18
3.3.1 Wazuh 19
3.3.2 Terminus 19
3.3.3 Nano 20
3.3.4 Typhoon 20
3.3.5 Ubuntu 21
3.3.6 Kali Linux 21
3.3.7 Hydra 21
3.4 Deployment Wazuh 22
3.4.1 Persiapan Kebutuhan Deploy Wazuh Manager 22
3.4.2 Desain Infrastruktur Wazuh Manager 24
3.4.3 Instalasi Komponen Wazuh Manager 24
3.4.3.1 File konfigurasi wazuh 25
3.4.3.2 Pengistalan wazuh indexer 26
3.4.3.3 Pengistalan wazuh server 27
3.4.3.4 Pengistalan wazuh dashboard 29
3.4.3.5 Ubah user dan password 30
3.4.3.6 Cek hasil instalasi wazuh manager 30
3.5 Penambahan Agen Wazuh 31
3.6 Mengaktifkan Fitur Vulnerability Test 32
3.7 Menambahkan Active Respons Untuk Mengatasi Brute Force SSH 34
3.7.1 Mendefinisikan ID rule brute force SSH 34
3.7.2 Active respons brute force SSH 35
3.7.3 Generating active respons 36
3.8 Pembuatan Wazuh Custum Dashboard 37
3.8.1 Custume dashboard vulnerability test 37

3.8.2 Custume dashboard brute force SSH 38
3.9 Ruang Monitoring Control 40
BAB IV HASIL DAN PEMBAHASAN 41
4.1 Hasil Akhir (Luaran) 41
4.1.1 Security Log Analysis 41
4.1.2 File Integrity Monitoring 42
4.1.3 Vulnerability Detection 43
4.1.4 Wazuh mengatasi brute force SSH dengan active respons 43
BAB V KESIMPULAN DAN SARAN 46
5.1 Kesimpulan 46
5.2 Saran 46
DAFTAR PUSTAKA 47
LAMPIRAN 48