

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN ORISINAL	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR	vi
LEMBAR PERSEMBAHAN	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
DAFTAR SINGKATAN	xiv
DAFTAR ISTILAH	xv
DAFTAR LAMPIRAN	xviii
BAB I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	3
I.3 Tujuan Penelitian	3
I.4 Manfaat Penelitian	3
I.5 Batasan Penelitian	4
I.6 Sistematika Penelitian	4
BAB II TINJAUAN PUSTAKA	6
II.1 <i>Vulnerability</i>	6
II.2 Virtualisasi	6
II.2.1 Virtualbox	6
II.3 Teknologi <i>Container</i>	7

II.3.1 Docker	7
II.4 <i>Content Management System</i>	8
II.4.1. Joomla.....	9
II.5 <i>Vulnerabilty Scanner</i>	9
II.5.1 Clair Scanner	9
II.5.2 JoomScan.....	9
II.5.3 Alasan Pemilihan <i>Tools Scanning</i>	10
II.6 <i>Operating System</i>	11
II.6.1 Lubuntu.....	11
II.7 <i>Tools Pengujian</i>	11
II.8. <i>Common Vulnerability Scoring System</i>	11
II.8.1. Definisi CVSS	11
II.8.2 <i>Base Score Metrics</i>	12
II.8.3 <i>Temporal Score Metrics</i>	13
II.8.4 <i>Environmental Score Metrics</i>	13
II.8.5 Kalkulator CVSS v.3.1	14
II.9 NVD NIST.....	14
II.10 Analisis Statistik Deskriptif.....	14
II.11 <i>CyberSecurity Framework</i>	14
II.12 GSA CIO-IT <i>Security-17-80</i>	15
II.13 Penelitian Terdahulu.....	16
II.14 Penelitian Terkini/Saat Ini.....	17
BAB III METODOLOGI PENELITIAN.....	18
III.1 Pengembangan Model Konseptual.....	18
III.2 Sistematika Penyelesaian Masalah.....	18
III.2.1 Tahap Perumusan Masalah	19

III.2.2 Tahap Hipotesis.....	19
III.2.3 Tahap Rancangan Pengujian.....	20
III.2.4 Tahap Implementasi.....	20
III.2.5 Tahap Analisis.....	20
III.2.6 Tahap Akhir.....	20
BAB IV RANCANGAN PENGUJIAN.....	21
IV.1 <i>Scanning Capabilities</i> : GSA CIO-IT Security-17-80.....	21
IV.1.1 <i>Hardware</i>	21
IV.1.2 <i>Docker Images</i>	21
IV.1.3 Joomla.....	24
IV.2 Skenario Pengujian.....	27
IV.2.1 Skenario <i>Vulnerability Scanning</i> pada <i>Docker Images</i> versi 1.....	28
IV.2.2 Skenario <i>Vulnerability Scanning</i> pada <i>Docker Images</i> versi 2.....	29
IV.2.3 Skenario <i>Vulnerability Scanning</i> pada Joomla versi 1.....	30
IV.2.4 Skenario <i>Vulnerability Scanning</i> pada Joomla versi 2.....	31
BAB V IMPLEMENTASI DAN HASIL PENGUJIAN.....	32
V.1 <i>Vulnerability Scanning Process</i> : GSA CIO-IT Security-17-80.....	32
V.2 <i>Vulnerability Scan Reports</i> : GSA CIO-IT Security-17-80.....	32
V.2.1 <i>Report Docker Images</i> Versi – 1.....	32
V.2.2 <i>Report Docker Images</i> Versi – 2.....	37
V.2.3 <i>Report Joomla</i> Versi – 1.....	42
V.2.4 <i>Report Joomla</i> Versi – 2.....	45
BAB VI ANALISIS.....	48
VI.1 <i>Documenting Report Reviews</i>	48
VI.1.1 Analisis Perbandingan Waktu Versi – 1 Dan Versi – 2.....	48

VI.1.2 Analisis Perbandingan Data Perubahan <i>Total Vulnerabilities</i> Versi – 1 Dan Versi – 2	49
VI.1.3 Analisis Perbandingan <i>Severity Level Vulnerability Scanner</i> dan Hasil Perhitungan CVSS	53
VI.1.4 Analisis <i>Closed Vulnerability</i>	55
VI.1.5 Analisis <i>Open Vulnerability</i>	59
VI.1.6 Analisis <i>Newly Vulnerability</i>	60
VI.2 <i>Remediation Verification : GSA CIO-IT Security-17-80</i>	62
VI.3 <i>Re-Classification of Known Vulnerabilities : GSA CIO-IT Security-17- 80</i>	66
BAB VII KESIMPULAN DAN SARAN	71
VII.1 Kesimpulan.....	71
VII.2 Saran	71
DAFTAR PUSTAKA	72
LAMPIRAN	75